SearchCompliance.com E-Guide

Compliance and Risk Management Strategy

As the worlds of security, compliance and risk collide, CIOs are increasingly approaching their information management responsibilities with a risk management lens. This E-Guide will look at how CIOs take a strategic approach to risk management and compliance and how to mitigate operational risks of outsourcing services. In addition, business model risk and how to define risks, core assets and establish acceptable levels of risk will be discussed.

E-Guide

Compliance and Risk Management Strategy

Table of Contents:

How to mitigate operational, compliance risk of outsourcing services

Richard E. Mackey, Contributor

Outsourcing services are a fact of life in today's business environment. However, while it may allow you to focus on what you do well and be more efficient, it can also bring both operational and compliance risk. This article discusses the importance of understanding the risk associated with third parties and how to manage this risk. The article provides guidance on how to recognize third-party operational and compliance risk and how to structure a provider management program to ensure that risk is assessed, understood, monitored and managed appropriately.

Operational and compliance risk

When an organization shares information with another organization, the risk of that information being compromised is increased. In other words, the organization has increased its operational risk. In addition, if the organization sharing the data has not taken the necessary steps to ensure that the information is protected appropriately according to the requirements of applicable regulations and contracts, the organization has increased its compliance risk.

Many regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act and the Massachusetts Identity Theft law (MA 201 CRM 17.00), require organizations to review their service providers' security practices and ensure that the information will be protected adequately. PCI -- a contract rather than a regulation or statute -- also requires merchants and service providers to ensure that service providers are compliant with the Payment Card Industry Data Security Standard in the functions they provide. Given these regulatory requirements, it is imperative that organizations have an organized approach to evaluating the type of risk a particular service represents, the level of risk of both the service and the provider, and the adequacy of the security practices of the provider in mitigating the risk of compromise and meeting compliance requirements.

What is at risk?

The first step in understanding risk is understanding exactly what information you are sharing. This may seem like a nonissue, but in many cases organizations share information in bulk without considering the individual data elements. Lack of data analysis can lead to unnecessary risk of exposure, increasing both the risk of compromise and the risk of being found noncompliant with contracts and regulations. Assuming you have analyzed the information to be shared, you can ask the following questions:

- Does the information include personal identifying information, healthcare data or credit card data?
- Is the information competitively sensitive for you or a business associate?
- What aspects of the information are sensitive? Is the confidentiality, integrity and/or availability of the information critical in the context of the service that you or your business associate provides?
- Does the data fall under requirements and restrictions specified by an existing contract?
- Is the data regulated by an agency or government statute?

If we look at a hypothetical example, we can see how understanding the information can help you measure the risks and understand requirements:

St. Fictitious Hospital shares patient records including names, Social Security numbers, addresses and treatment data with HealthService Inc., a service provider that allows doctors to view and approve treatment records for submission of claims to insurance companies. The hospital recognizes that as a covered entity under HIPAA it is required to protect the confidentiality, integrity and availability of Electronic Protected Health Information. In the case of insurance claim submission, the confidentiality and integrity of the records are more important than the immediate availability. Consequently, the hospital needs to ensure the effectiveness of the controls that affect those aspects of the information.

The hospital also recognizes that there is a chance that some patient is a resident of Massachusetts, therefore it will assume that its controls and the controls of the service provider must meet the requirements of the Massachusetts Identity Theft Law. Both laws require the hospital to assess the adequacy of security practices of business associates to which they entrust this protected information. In HIPAA parlance, the "covered entity" (the hospital) must ensure that all the administrative and technical controls are implemented by the business associate (HealthService), including appropriate encryption on transmission on unprotected networks, strict access controls on the data and disciplined vulnerability management.

Interestingly, the Health Information Technology for Economic and Clinical Health Act (HITECH Act) has brought additional pressure on business associates. In the past, HIPAA violations and compliance were the responsibility of the covered entity. The HITECH Act expands the responsibility of business associates, making them directly responsible for the safekeeping of the data. This change makes the Massachusetts law and HIPAA consistent in that organizations are responsible for any data they possess, regardless of how they acquired it.

The hospital will then need to go through an organized process of evaluating the business associate's practices and requiring improvements wherever they fall short. If possible, the hospital should also look to anonymize or eliminate any data that is not necessary to be shared. This practice can mitigate risk substantially.

Inherent vs. residual risk

As we have said above, all relationships bring some degree of operational and compliance risk. However, not all relationships are created equal. Two of the most critical elements in managing partner risk are consistently assessing the inherent risk associated with the shared information or relationship and assessing the residual risk of dealing with a particular partner in the context of its implemented controls.

The first element, assessing inherent risk, requires you to look at the data shared and the effect a compromise would have on your business and state of compliance. You assess the relationship assuming no controls. This is a worst-case analysis of the damage you would suffer in the event of a breach.

This analysis allows you to rank, by risk, the service providers you deal with based on the criticality of the information you share and the service they provide. Based on this analysis, you can then determine the depth of assessment you need to conduct to assure that your risk is mitigated appropriately.

The inherent risk analysis allows you to establish tiers: high-risk, medium-risk and low-risk service providers. This ranking will allow you to devise appropriate assessment methods that are commensurate with the risk. Low-risk partners may not require an assessment at all or may be required to only sign agreements accepting responsibility for whatever risk exists.

Medium-risk providers may be required to answer a security practices questionnaire and only be investigated in more detail if their answers raised concerns. High-risk providers might be required to submit a third-party audit report or undergo a detailed assessment by your internal security group.

This tiered system not only allows you to closely inspect your highest-risk partners, but it also helps you mitigate both operational and compliance risk. The initial assessment in a relationship lays the groundwork for future periodic reviews that are required by many contracts and regulations (and simply make sense).

The ongoing partner management program

When you have established a relationship with a partner, your risk management responsibility has only begun. As time goes by, the risk associated with a given service changes substantially as a result of changes to your business, your partner's business, your technology, the threat environment or new regulatory or contractual requirements. Consequently, the risk associated with every service relationship needs to be re-evaluated periodically to both recognize and adapt to these changes.

The risk-based tier system can help maintain your partner risk management program by helping to set the frequency of your periodic risk assessments and partner practice evaluations.

The risk-based tier system can help maintain your partner risk management program by helping to set the frequency of your periodic risk assessments and partner practice evaluations. The higher the risk associated with a given partner the more frequent your risk and practice assessments should be.

When planning your risk assessments, keep in mind that you need to understand whether changes in your partner's environment have an impact on your risk. For example, has your partner gone through a merger or acquisition? Has your partner's technical environment changed in important ways? Is your partner aware of regulatory requirements and changes that have occurred in the time since the previous review?

These questions can only be answered by communicating with your partners. This is a critical component of any partner management program.

Virtually all companies engage third-party service providers. We know that these relationships bring with them certain types of risk. It is critical that we understand these risks and manage them, not only at the initiation of the relationship, but also throughout its existence. A well-run, consistent and methodical risk-based partner management program should be part of all organizations' security and compliance programs.

Richard E. Mackey, vice president, SystemExperts Corp., ISACA/CISM is a leading authority on enterprise security architecture and compliance.

Strategic risk management includes risk-based approach to compliance

By Linda Tucci, Senior News Writer

Ask "What is strategic risk management for compliance?" and the answer will depend on who's talking. But the gist is this: Rather than allowing the ever-multiplying regulatory mandates to determine a compliance program, an organization focuses on the threats that really matter to its business -- operational, financial, environmental and so on -- and implements the controls and processes required to protect against them.

"You need to do information security not to meet compliance but to protect the business. There is a huge difference between those two methodologies," said Candy Alexander, chief information security officer (CISO) at Long Term Care Partners LLC, an insurance company formed in 2002 to provide long-term care insurance and administer medical benefits for federal employees.

Alexander practices what's known in compliance circles as a risk-based approach to regulatory mandates, as opposed to compliance by checklist. Her risk management strategy focuses on three regulations: the Federal Information Security Management Act of 2002 (FISMA), the data privacy laws enacted by 44 states and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

But dare to suggest these big three mandates drive her organization's security strategy, and Alexander sets the record straight.

"I have been in organizations where my main focus was to meet compliance, nothing more, nothing less. People who are doing security for compliance purposes are putting their organizations at risk," Alexander said. Regulations, she added, should be the baseline.

Focusing on protecting the business will result in a strategic risk management program that, in theory, will answer compliance regulations but in some cases go well beyond the mandate. A risk management approach, say advocates, also saves money by reducing the redundant controls and disparate processes that result when companies take an ad hoc approach.

The scope of protection against threats and degree of compliance depends on an organization's risk appetite. The appetite for risk can wax and wane, depending on externalities such as a data breach, a global economic crisis or an angry mob of customers outraged by executive pay packages. When companies are making big profits, they can spend their way out of a compliance disaster. In financially rocky times, however, there is much less margin for error.

IT pros like Alexander and a variety of experts suggest that while a risk-based approach to compliance might be the right thing to do, it is also difficult, requiring that the organization:

- Define its risk appetite.
- Inventory the compliance obligations it faces.
- Understand the threats that put the various aspects of the business at risk.
- Identify vulnerabilities.
- Implement the controls and processes that mitigate those threats.
- Measure the residual risk against the organization's risk appetite.
- Recalibrate its risk appetite to reflect internal and external changes in the threat landscape.

A risk-based approach to compliance requires a certain level of organizational maturity and, some experts hasten to add, is ill-advised for young companies.

Strategic risk management for compliance can be managed manually or by Excel spreadsheets, but vendors promise that sophisticated governance, risk and compliance (GRC) technology platforms will ease the pain. Meantime, those baseline compliance regulations still need to be met to an auditor's satisfaction.

Do you know what level of risk your organization can tolerate?

The assumption in a risk management approach to compliance is that the business knows best about the risk level it can tolerate. But there's the rub, said Eric Holmquist, a risk management expert.

"When it comes to risk management, getting your head around a tolerance level is extremely difficult," said Holmquist, former director of operational risk management at Advanta Bank Corp.

Then there's the dirty little secret of every organization: "For hundreds of years, businesses have been managing risk intuitively: I perceive there to be a risk; therefore I build control. But most controls are built to a perception of the risk and a perception of the scope of the risks, without really stopping to consider what is the real risk and is this the right control," he said.

By not doing the risk-benefit analysis, companies get the controls wrong. "I can't tell you how many times I've seen a $1 million control mitigating a $100,000 risk," Holmquist said.

The short end of the cost-benefit analysis

Back in the 1970s, Ford Motor Co. was sued for allegedly making the callous calculation that it was cheaper to settle with the families of Pinto owners burnt in rear-end collisions than to redesign the gas tank. The case against Ford, as it turns out, was not so cut and dried, but the Pinto lives on in infamy as an example of a company applying a cost-benefit analysis and opting against the public's welfare.

"Regulations introduce externalities that risk management itself would not have brought to bear," said Trent Henry, a security analyst at Midvale, Utah-based Burton Group Inc. "Regulations make it a cost of doing business."

A recent example concerns new laws governing data privacy. For many years in the U.S., companies that collected personally identifiable information owned that data. In the past, losing that information didn't hurt the collector much but could cause great harm to the consumer, Henry said, "hence the regulations." But the degree to which a business decides to meet the regulation varies, depending -- once again -- on its tolerance for risk. Organizations must decide whether they want to follow the letter of the law to get a checkmark from the auditor, Henry said, or more fully embrace the spirit of the law.

"Is your philosophy as an organization minimal or maximal? And if it is minimal, you may decide that it is worth it to get a small regulatory fine rather than comply," he said.

Indeed, "businesses now are cutting costs so narrowly that some know their controls are inadequate and are choosing not to spend that $1 million to put the processes, the people and infrastructure in place for that $100,000 fee," Henry said, echoing Holmquist. "They calculate they're still $900,000 ahead." But don't expect a business to own up to that. "They never let that cat out of the bag."

Sarbanes-Oxley drives risk management strategy

Compliance is expensive. It is hardly surprising that companies are looking for ways to reduce the cost of regulatory compliance or, better yet, use compliance to competitive advantage. According to Boston-based AMR Research Inc.'s 2008 survey of more than 400 business and IT executives, GRC spending totaled more than $32 billion in 2008, a 7.4% increase from the prior year.

The year-over-year growth was actually less than the 8.5% growth from 2006 to 2007, but the data shows that spending among companies is shifting from specific GRC projects to a broad-based support of risk. In addition to risk and regulatory compliance, respondents told AMR they are using GRC budgets to streamline business processes, get better visibility to operations, improve quality and secure the environment.

"In prior years, compliance as well as risk of noncompliance was the primary driving force behind investments in GRC technology and services. GRC has emerged as the new compliance," AMR analyst John Hagerty said.

Folding regulatory mandates into the organization's holistic risk management strategy gained momentum in the wake of the Sarbanes-Oxley Act of 2002 (SOX), one of the most expensive regulations imposed on companies. SOX was passed as protection for investors after the financial fraud perpetrated by Enron Corp. and other publicly held companies, but it was quickly condemned by critics as a yoke on American business, costing billions of dollars more than projected and handicapping U.S. companies in the global marketplace.

Indeed, the law's initial lack of guidance on the infamous Section 404 prompted many companies to err on the (expensive) side of caution, treating the law as a laundry list of controls. By 2007, under fire from business groups, the Securities and Exchange Commission and Public Company Accounting Oversight Board issued a new set of rules encouraging a more top down-approach to SOX.

"There are certain areas mandated you wouldn't want to meddle with -- it is legal and no exceptions -- but instead of checking every little box, companies were advised to take a more risk-based approach," said Ravi Shankar, head of assurance services at Capgemini's business process outsourcing division in Bangalore, India.

Risk management frameworks and automated controls

Risk management frameworks are not new, and neither, really, is a risk-based approach to compliance, Shankar points out. But the strategy has been gaining ground, driven in large part by IT as well as by IT best practices frameworks such as COBIT and the IT Infrastructure Library.

Ten years ago at any well-managed organization, 75% of controls were manual. "Today, the industry benchmark is the other way around. IT drives about 70% of the controls and 30% are manual." The endpoint is to move the 30% manual controls to automated controls, Shankar said.

Two fundamental building blocks are essential to adopting a risk-based approach to compliance, in Shankar's view: stable systems and processes, and a strong business ethos. "If a company has absolutely diverse processes, it is not a good choice," he said. Burton Group's Henry concurred. "It's more like crisis management than risk management for those guys -- compliance Whack-a-Mole."

Formulating a strategic risk management strategy also requires a clear definition of the values and principles that drive the organization's business -- in other words, a certain level of maturity, Shankar said. "If the ethos is loosely defined, then it is not safe to take a holistic approach to compliance."

Companies that make the grade, that give consistent guidance to investors, indeed any that operate successfully in the SOX arena, are probably ready for a risk-based approach, Shankar said.

GRC management software

Shankar gets no argument on that point from Alexander Paras, who joined LeapFrog Enterprises Inc. in 2006 to manage the educational toy maker's SOX compliance. LeapFrog recently bought GRC management software from BWise to support SOX compliance and manage enterprise risk.

"What did we have before? We had a nightmare! We had a bunch of Excel schedules and Word documents and Microsoft Project to manage things," said Paras, senior manager for compliance at Emeryville, Calif.-based LeapFrog until March 2009, when he was named divisional controller for the company's Mexico division. "As you can imagine from a version control standpoint, this created quite a bit of frustration for the auditors, business process owners and senior management."

LeapFrog needed greater transparency into its compliance efforts and controls. Unlike come of the other 20 solutions vetted, BWise GRC works at a process level, Paras said, capturing changes as they are made to documents and automatically ensuring those changes are reflected in all the other relevant systems in the compliance process.

People who are doing security for compliance purposes are putting their organizations at risk.

Candy Alexander
CISO, Long Term Care Partners LLC

"You have one point of contact in the system and all the information cascades down," Paras said. "SOX is just part of the routine, rather than an onerous project, which is what it should be."

Luc Brandts, BWise founder and chief technology officer, said the starting point for most customers is money. "GRC to improve business is a great story, but we come in to solve a pain point. The cost of compliance is too high. Customers see they are doing the same thing eight times and want to get a grip on this, and as a second result they get a grip on their business. In the process they find out they have 16 different ways of doing accounts payable and there is no reason on earth to do so."

In an era of increasing regulation and more guidelines likely on the way, companies might be excused for seeing the auditor as the next threat. But don't tell that to Long Term Care Partners' Alexander, who got her start at Digital Equipment Corp. (DEC) "in the days before there were regulations." Security folks had to jump up and down to try to get the business to protect information. "And they would say, 'We really don't need that, or there is no ROI.'"

DEC quickly learned the value of data protection after its source code was stolen by notorious hacker Kevin Mitnick, she says. But the response from the business side was often that it would take the risk -- to an absurd degree, Alexander recalled.

"That risk acceptance level was getting higher and higher and higher until it got to a ridiculous point, and that is when they came out with these regulations, with HIPAA, with Gramm-Leach-Bliley, with FISMA. A lot of folks in the security business went, 'Phew! At least now we can get it done.'"

Business model risk is a key part of your risk management strategy

Business model risk probably is not always the first application of risk management that C-level officers or IT administrators think of, as they are usually more concerned with risk management as it applies to security or compliance. Amit Sen, director and practice leader at Patni Americas Inc.'s business consulting services group, and John Vaughan, director of industry solutions in the group, have a different view on the importance of business model risk, and they spoke with SearchCompliance.com Executive Editor Scot Petersen about the subject. The transcript that follows includes extended excerpts from a Compliance Advisor podcast recorded this week.

This interview continues our discussion from a few weeks ago, when I met Amit and John at the MIT Sloan CIO Symposium. We were in the "IT Governance, Risk and Compliance" panel. During the Q&A period, John asked the panel if they thought that risk management was too focused on security. A few of the panelists danced around the question and never answered it. Later, I asked John if he thought the panel had answered his question. So John, let me start with you. What you trying to ask the panel that day, and what did you think of their answer?

Vaughan: We were at MIT and we had some heavyweights on the panel. One was from the SEC [David Blaszkowsky] and another from Sallie Mae [Karen Kotowski]. We were talking about this idea of governance, risk and compliance.

It sounds so important. But we just came through financial crisis where people or companies were not watching risk, which is the middle term. My primary question was that the last seven years of IT strategies around SOX [Sarbanes-Oxley] compliance seemed to be very focused on security, and hardening the assets and making sure who has the data, and who could see the data. But at the end of the day that does not address the systemic risk that businesses are facing, and how do you get companies to focus more on looking at risk to their business models -- not necessarily risk to what is essentially breaking and entering, or unauthorized access to data. And the panel just didn't know how to answer that.

I think they've been deeply entrenched in the spirit of trying to create security and maybe transparency in reporting, but there hasn't been much focus on putting my business model at risk. And we thought it was a very appropriate topic. [Most executives] talk about process automation, and how process automation is taking business processes and automating them, and then you think about risk. And the question we're trying to pose to the industry is can we take the maturity of a GRC process and turn it onto business model risk instead of security or procedure risk so we can adopt a mature process that already has the CIO's attention, and say, we would like to focus this process, and now let's look at risk to the enterprise business model. Are there things we're doing to automate or going to automate; are there automation changes we are doing that can accelerate the risk to our business model.

In the world of manufacturing you don't have to look very far below the surface to see that people have automated processes that are losing the company money or creating additional risk, and we would like to introduce into the IT governance stack this idea of what procedures can we put in place so that we are watching whether these new things we're automating create risk for the business model. So it's one of those questions: Yes, IT could do it, put

up a website, form partners with third parties, and you could connect everybody. But are you introducing risk to the core business model of profitability and market share and leverage. If you take that same process and put a checkmark on it, and go, "I'm going to watch business model risk as part of this process," then I think you really start to address the concerns that were raised when they created the Sarbanes-Oxley legislation, which is not only how do you get more transparency, but you really are trying to answer the question, how do you reduce the chance of a catastrophic failure due to unseen business risk.

Amit, do you think that risk managers can really spend too much time on security?
Sen: The root question is, what is risk, how does risk get introduced by IT or in an IT platform process? And is it about securing the gates or is it about securing the causes that introduce risk that impacts your business model. Or do we primarily focus on password reset and physical risk and security management?

The problem that has happened is IT has become very complex. IT has become global. IT is supporting global platforms, global processes. And IT-enabled processes now have exposure simultaneously to everywhere in the world. So even two to three years ago, if there was ineffective IT governance, if they didn't pay enough attention to risk, the impact was limited so you had some time to react.

Because of lack of management, of complexity that IT introduces in the system, a lot of times transparency is an issue. People do not know what business processes have been automated, what is the implication of turning on the switch and taking the process global? They do not understand how the applications are connected; they do not understand how the data is defined. So the question fundamentally comes down to what are we securing against? Is it only about separation of duties? That's kind of what Sarbanes-Oxley has forced IT organizations to do. But sometimes they have missed the bigger picture.

We talk about globalization and this world of connected systems. There have been situations where companies have run a promotion globally without understanding the impact it will have on the supply chain. So their system got so overwhelmed that they realized within the first two hours of running promotion that this was going to be such a tremendous financial disaster for them, they had to put an immediate stop to that. Did they realize and understand before they actually went into this what the implications were, how quickly the impact of this would be felt everywhere within in the organization? That is fundamentally where we come from. There is something about physical security, IT security, data security, application security that we have to worry about. However, we need to remind the executives, the IT executive, the business executives, that the lack of effective IT governance, lack of desire to control the complexity within IT systems, portends a much bigger risk and much more disastrous risk to your organization than what you have to do as part of Sarbanes-Oxley.

When applying risk management to business processes, how is this accomplished? How do we measure this risk, and then how can companies interpret that data?
Vaughan: You have to start with ensuring that the company clearly builds their own model and documentation around what their business model is. So if you're a CPG [consumer packaged goods] company and you are shipping products, your business model revolves around manufacturing, market share, profitability and inventory positions. And anything that affects your inventory position, or market share, or anything that affects the profitability of those shipments, needs to go through a GRC check. And you have to model the impact of it.

We're trying to push companies to get out of anecdotal and into modeling. If you are going to change your distribution network, as another example, we had one scenario where the guy says we want to ship every product from anywhere. But if you give them the freedom to ship any product from everywhere, you create chaos in the supply planning system. And there are other little items inside of all these systems that directly affect the model.

Sen: If we look at that from a framework point of view, what is it we need to establish? The first thing to establish is a foundation, an understanding of the current infrastructure, current applications and business process and how they're implemented. The second leg in the framework is a process that's a change-management process or overall risk management process that has IT as a core participant in the process and that is managed and addressed globally. The third thing is to create a risk-awareness culture. Sometimes people tend to forget IT organizations as a significant player in managing the risk in an organization. That has to change, and IT people responsible for IT applications and processes have to be included and get more aware of what a risk awareness culture is and how that brings value.

So when you model risk, are you taking a worst-case scenario, or is there some amount of risk that's acceptable here?

Vaughan: Anytime you introduce a change, you do risk vs. reward. So what we recommend is, they have to understand what the core levers in your business model are. So if you are a wholesaler, maybe it's break bulk [shipping]; banks, it's around leverage. You have to know what your key lever points are. You really have to model it. If it's too complex to model it, you have to reach out. We formed a partnership with some folks at MIT. So if we have a business model that someone wants to make changes to or change the automation system, and it's very complex and global, we'll reach out to a research partner. So you just have to make sure that the change you're going to make really is backed up by, one, where's the industry headed; and two, what the research shows; and three, we see that it does not introduce new risk into the business model.

I don't think you ever want to increase the risk on the business model. All of your projects should focus on reducing the existing risks and costs. You have to do it empirically and understand what really happens. … I wouldn't take on many programs that introduce risk to a core business model. The whole point of bringing up the GRC process, if you put a process in place, you understand which ones increase risk and which ones reduce risks. But most of the IT people running those process automations don't understand whether or not they're increasing risk. All they are trying to do is deliver on requirements.

Sen: Can there be life without risk? I don't think that's necessarily possible, or desirable. However, what we need to understand is where are we are introducing risks, and the risk is understood and planned and not a byproduct of a lack of knowledge or visibility into what actually goes on in the organization. We find time and again that the IT organization is not well integrated into this process. Overall risk management and risk mitigation is still not taken seriously.

Who leads this process? Is this outside of IT and if so, what kind of relationship does that person have with IT?

Vaughan: We're at a unique point of history. What's happened in the last 10 years is you have an IT landscape that is dominated by ERP solutions, which drive a lot of process automation. You've actually done a transfer of

knowledge from the business department into the IT department of how the business is actually running. You end up with a lot of the process knowledge in the IT department now because they are so tied into these pieces of software that we feel the leadership has to come outside of the realm of IT. They really own the process now, because that's what runs. You can automate a process that could cause you to lose money for years and may not know it, there's so much data. We're trying to adapt, so that if you take the strength of GRC, it should have roles in product portfolio and management. What we'd like to do is adapt that role to look at business model risk. We would team up with either an outside consultancy or an outside research partner like we have been able to do with some of the universities, so you can produce an independent voice on what's going to happen to the business model when changes are introduced.

What we need to understand is where are we are introducing risks, and the risk is understood and planned and not a byproduct of a lack of knowledge or visibility into what goes on in the organization.
Amit Sen
director and practice leader, Patni Americas Inc.

Sen: There's talk in our industry now: Is the role of the CIO changing. To me it has already changed. The CIO is more of a "CPO," a chief process officer. That has always been the true role of the CIO. Because of ERP and wide adoption of ERP applications, that is the single most important role in any organization that truly has an end-to-end view of what actually goes on in an organization. They also have the data they can pull in; they can slice and dice and look at the processes going on, and all the implications that come with it. It's time to make that to a certain extent formal and responsible to not only execute a process, but truly understand the implication of it on the business model ... and enable the organization to understand the risk and react to it. It has to start with the CIO's office, but it needs the proper alignment with the rest of the executive team. And there has to be visibility of this at the board level as well. There's a certain level of education that has to happen, and the responsibility lies with the process and an understanding that what really goes on is really there.

When you introduce partners into this process, do you have to introduce a separate process, some kind of a partner management program, to vet them for the kind of risk they would introduce into the system or to the business model?
Vaughan: Yeah, you definitely need to box your partners in, in a way that they can perform services well for you. Most IT projects or initiatives have a couple very strong sponsors. Those sponsors have bought into a vision, so what you are trying to do is introduce some kind of objective third party, whether it's the GRC office itself or a research firm or a consulting firm to vet it out and make sure it doesn't impact the model. You have to have a special relationship with those partners to make sure that [the relationship] is not accelerating risk.

At a minimum, we want people to actively manage it so it doesn't look like a due diligence problem. … We're just trying to say we need to be more careful with our automation process and we really need to benchmark them against their effects on the core business model. And if you do see risk you have to manage them. So the metrics have to be defined up front, and how do you incent people to succeed when it's a function you had and then you outsourced.

Sen: IT risk is business risk. Businesses can't afford to assume IT risk is contained within the IT walls. As we go through this process of replacing a technology-driven approach and a fragmented view of IT risk with more of an integrated view, that starts the understanding of the business risk and consequences that come from certain IT decisions. Three thoughts I want to leave everyone with: Beef up your IT governance. A lot of our understanding, or lack of, starts there. No. 2: Manage complexity of your processes and systems, so it's easier for the IT organization to understand business issues. And three, create a risk-aware culture, that there are certain business impacts that happen from certain [IT] decisions or the things they undertake.

Resources from Ounce Labs, an IBM Company

Meeting the PCI Application Security Requirements

Compliance Guide

PCI Compliance at the Source

Customer Case Studies on Applications Security

Podcast: What, How & Why of AppSec-Keeping up with Evolving Compliance Guidelines

Podcast: Judging PCI Compliance

General information on compliance can be found here:

About Ounce Labs, an IBM Company
Ounce Labs, acquired by IBM in July 2009, delivers the industry's leading Static Application Security Testing (SAST) suite bringing enterprise-wide awareness of business critical vulnerabilities. With this ability to identify and prioritize security issues, organizations have the information they need to address their greatest risks throughout the SDLC. Ounce's patented source code analysis delivers the scalability and automation to help organizations strengthen application security and protect confidential information. Ounce Labs, an IBM company, also helps organizations to verify regulatory and policy compliance, addressing PCI DSS, FISMA, HIPAA and others. For more information, please visit www.ouncelabs.com.