

Governance, Risk, Compliance

POLICY MANAGEMENT: METHODS AND TOOLS

IT managers are looking to governance structures and the discipline of risk management to help them make decisions and create sustainable processes around regulatory compliance.

CHAPTER 1:

Risk Management: The Right Balance

CHAPTER 2:

A Risky Approach

CHAPTER 3:

Buyer Beware: The Complexities of Evaluating GRC Solutions

Risk Management: The Right Balance

Information security is a business issue
and not an IT issue, and must involve
a cross-functional approach.

BY ERIC HOLMQUIST



CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE



CHAPTER 2
A RISKY
APPROACH



CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

ONE OF THE most critical components of any information security program is the risk assessment. It is also one of the most misunderstood and poorly executed.

In truth, a good information security program is not based on one risk assessment, but a series of them at various levels of granularity. For instance, an organization with Web servers is likely to hire an outside security firm to perform a specific vulnerability assessment on those servers. But every organization, regardless of size, complexity or business model, should have a core, enterprise-wide information security risk assessment that is foundational to its risk management activities.

This “foundational” aspect highlights one of the central challenges of developing this risk assessment, and that is the tension between managing risk by “intuition” versus by “fact.” This is particularly pronounced in the

field of information security, because there is a perception that the risk is obvious—that the data could be compromised. Therefore, people often have a tendency to build controls based largely on their perception of the risks without fully analyzing exactly where the risks are and then focusing a commensurate amount of mitigating activities on those areas.

A holistic, risk-based approach to managing information security (IS) will *always* be a balance between intuition and some sort of framework. The challenge is in finding that balance and using a framework that is relevant, culturally acceptable and actionable. The purpose of this article is to outline one framework for assessing information security risk based entirely on awareness and accountability.

The worst possible approach that an organization could take in developing an information security risk

↳
CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

↳
CHAPTER 2
A RISKY
APPROACH

↳
CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

assessment would be to task it to IT to develop. Information security is not solely an IT issue; it is a business issue and must be managed that way. In that light, the first structural elements of the information security risk assessment are the focal points, which are:

- Information systems (IT)
- Electronic data (business heads)
- Physical files (department heads)
- Third parties (relationship owners)

What is critical to note here is that each of these four areas has a *distinctly different owner*. It is reasonable to ask IT to take ownership of the internal systems and to assess the inherent risk to those systems. The other three areas, however, are each represented by unique business owners.

Whereas IT should be asked to document and assess the systems infrastructure, this is different than the actual data. It would be unreasonable to expect the IT staff to be in every case intimately aware of exactly what data is being populated into every data source, particularly things like analytic and ad hoc reporting databases. Instead, these should have specific business owners that can identify the use and content of every database.

Likewise, department heads must be responsible for documenting what they maintain in physical files within

their respective areas and third-party business owners must be responsible for certifying their third parties in terms of what information is shared with them and what controls are utilized by those third parties.

When viewed in this context, it becomes immediately obvious why information security is a business issue and not an IT issue, as it must involve a cross-functional approach.

Next, in terms of developing a rough calculation of actual information security risk, the following methodology is one I have developed over the years, which has proved fairly effective as a tool to help prioritize efforts and validate the application of internal controls. IS risk can be generally grouped into four broad categories:

- What is at risk?
- What would be the impact?
- What could be the source?
- What can we mitigate?

We'll look at each one of these briefly to consider the parameters to be evaluated and how these factors contribute to an overall risk score.

What is at risk? This is the data categorization step. Every organization should utilize some form of data categorization strategy to help define its data sources. In my model I use five categories: Customer/applicant, corporate, operational, prospect and

↳
CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

↳
CHAPTER 2
A RISKY
APPROACH

↳
CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

third party. Within each of these I use a subcategorization of *confidential*, *sensitive* or *public* to indicate level of confidentiality. Therefore, we first ask *how much* and *what type* of data resides within any given system, database, physical area or third party. These “quantity” plus “sensitivity” values create the first data point.

What would be the impact? The second factor is an impact factor in the event of a data compromise. This category is made up of four criteria: Financial, operational, regulatory and reputation. The score in this case represents the degree of impact within each of those four criteria, which would be somewhat dependent on the data categorization but may consider other factors as well.

What could be the source? This category contains five values: a person inside the company, a person outside the company, a system inside the company (that, say, malfunctioned, inadvertently exposing data), a system outside the company and a natural disaster. Within this category the weight factor is the degree of likelihood, which is represented both by the number of people or systems involved (the more people accessing a given database, the more source risk there is) as well as some estimate of the likelihood of something going wrong. This is the assessment category that is used to capture things like

systems vulnerabilities as well as scope of data access.

What can we mitigate? Finally, whereas the previous three areas provide an increase in risk scores, this area reduces those scores. The three aspects of mitigation are prevention, monitoring and recovery. Unfortunately, the best that one can usually expect is a high score under prevention, a moderate score under monitoring (since some data movements can be monitored) and virtually no score under recovery, since once the data is gone, it’s gone and you’re not going to get it back.

The important thing to remember is the goal is not to develop a perfect risk score. The goal is to understand which systems, databases, physical environments and third parties are riskier than others, which should provide a basis to prioritize controls and risk management activities.

The fact is there is no perfect model for assessing information security risk. The key is to develop *something* and use it to create dialogue. The real value in this exercise is not necessarily the numbers that are produced, but the awareness that it creates in researching and analyzing data sources and potential risks. Anything that increases awareness and accountability is a good thing. ■

Eric Holmquist is a consultant and former director of operational risk management at Advanta Bank Corp. Write to him at echolmquist@verizon.net.

Three **critical** questions...

- o How secure & compliant is my network?
- o What are the top 10 things we need to do?
- o Who is accountable & how are they doing?

One **Suite** answer.



nCircle Suite360[™]
The Leader in Security & Compliance Auditing

Get the reports your boss wants:
www.ncircle.com/answer

nCircle^o

A Risky Approach

A risk-based methodology to regulatory mandates is all the rage in compliance circles, but it's not for beginners.

BY LINDA TUCCI



CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE



CHAPTER 2
A RISKY
APPROACH



CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

WHEN CANDY ALEXANDER lists the compliance obligations of the Greenland, N.H., insurance company where she runs security, she homes in on the Federal Information Security Management Act of 2002 (FISMA). That's because Long Term Care Partners LLC, formed in 2002 to provide federal long-term care insurance and administer medical benefits for federal employees, is a U.S. prime contractor.

"If we are not compliant with FISMA we don't run the business," says Alexander, chief information security officer at Long Term Care Partners, owned jointly by Boston-based John Hancock Life Insurance Co. and New York-based Metropolitan Life Insurance Co. "That's our first and foremost compliance driver."

Ranking second on Alexander's list are the data privacy laws enacted by 44 states. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) comes in a close third. 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 says. Regulations, she adds, should be the baseline.

Alexander practices what's known in compliance circles as a risk-based approach to regulatory mandates, as opposed to compliance by checklist. What constitutes a risk management strategy for compliance differs depending on who's talking. But the gist is this: Rather than allowing the ever-multiplying regulatory mandates to determine its 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,” Alexander explains.

PROTECTING THE BUSINESS FROM RISK

Focusing on protecting the business will result in a risk 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 might be the right thing to do, it is also difficult, requiring:

- Defining the organization’s risk appetite.

- Inventorying the compliance obligations facing the organization.
- Understanding the threats that put the various aspects of the business at risk.
- Identifying vulnerabilities.
- Implementing the controls and processes that mitigate those threats.
- Measuring the residual risk against the organization’s risk appetite.
- Recalibrating the organization’s 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. Risk-based compliance can be done 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.

\$1 MILLION CONTROL FOR \$100K WORTH OF RISK

The assumption in a risk management approach to compliance is the business knows best about the risk level it can tolerate. But there’s the rub, says Eric Holmquist, a risk man-



CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE



CHAPTER 2
A RISKY
APPROACH



CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

CHAPTER 2
A RISKY
APPROACH

CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

agement expert.

“When it comes to risk management, getting your head around a tolerance level is extremely difficult,” says Holmquist, former director of operational risk management at Advanta Bank Corp. Then there’s the dirty little secret of every organization, he adds.

“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.”

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 says.

That’s putting a good face on it.

PAYING THE PRICE: HOW MUCH IS BEING SPENT ON IT?

A look at where regulatory compliance requirements spending fits into the overall IT budgets for North American (NA) and Europe, Middle East and Africa (EMEA) companies:

PERCENTAGE OF 2006 BUDGET ALLOCATED TO:	NUMBER OF EMPLOYEES			
	EMEA <10,000*	NA <10,000	ALL EMEA 10,000+	ALL NA 10,000+
Transforming the business	16.29	11.34	17.61	13.38
Strengthening competitive position	12.08	11.48	12.86	11.97
Improving productivity and efficiency within IT organization	13.63	12.34	12.91	11.37
Improving productivity and efficiency outside IT organization	12.91	12.88	11.92	11.67
Operations (running and supporting the business)	15.79	27.89	15.75	25.9
Maintaining/improving IT staff skills	10	7.1	9.06	6.13
Meeting regulatory requirements	9.62	7.64	9.87	9.92
Maintaining/improving information security	9.44	9.07	9.73	9.39
Other	0.25	0.25	0.28	0.28

SOURCE: GARTNER INC. SURVEY OF IT MANAGERS (JANUARY 2007)

↳
CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

↳
CHAPTER 2
A RISKY
APPROACH

↳
CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

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 welfare.

“Regulations introduce externalities that risk management itself would not have brought to bear,” says 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 says, “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 says, 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 says.

Indeed, “businesses now are cutting costs so narrowly that some

“I can’t tell you how many times I’ve seen a \$1 million control mitigating a \$100,000 risk.”

—ERIC HOLMQUIST, CONSULTANT

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 says, 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.”

SOX DRIVES RISK MANAGEMENT STRATEGY

Compliance is expensive. It is hardly surprising that companies are looking for ways to reduce the cost of 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,

↳
CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

↳
CHAPTER 2
A RISKY
APPROACH

↳
CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

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 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,” says AMR analyst John Hagerty.

Folding regulatory mandates into the organization’s holistic risk 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

“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.”

—JOHN HAGERTY,
ANALYST, AMR RESEARCH INC.

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,” says Ravi Shankar, head of assurance services at Capgemini’s business process outsourcing division in Bangalore, India.

STABLE PROCESSES VS. COMPLIANCE WHACK-A-MOLE

Risk management frameworks are not new, and neither, really, is a risk-based approach to compliance,



Let them
roam
lose laptops
surf
audit
cut budgets

who cares **You do!** Liberating your people and freeing up time and resources makes productive sense. Sophos security and data protection solutions deliver: Install, set and forget. Easy on your time, easy on your system and easy on your business, everything from Endpoint to Compliance, Email, Web and Encryption is covered and all accessed and controlled with refreshing simplicity.

Now, with security taken care of, you've got the rest of the day to do all the other things that can't wait.

See for yourself – [learn more about Sophos today.](#)

SOPHOS
simply secure



↳
CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

↳
CHAPTER 2
A RISKY
APPROACH

↳
CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

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 says.

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 says.

Burton Group’s Henry concurs. “It’s more like crisis management than risk management for those guys—compliance Whack-a-Mole.”

Formulating a sound risk 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 says. “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 says.

A GLIMPSE INTO THE TOOLBOX

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 docu-

“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.”

—ALEXANDER PARAS,
DIVISIONAL CONTROLLER, MEXICO
DIVISION, LEAPFROG ENTERPRISES INC.

ments and Microsoft Project to manage things,” says 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

↳
CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

↳
CHAPTER 2
A RISKY
APPROACH

↳
CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

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 says, 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. “You have one point of contact in the system and all the information cascades down,” Paras says. “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, says 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.”

THE GOOD OLD DAYS—NOT!

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

“GRC to improve business is a great story, but we come in to solve a pain point. The cost of compliance is too high.”

—LUC BRANDTS, FOUNDER AND CTO, BWISE

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 recalls.

“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.’” ■

Linda Tucci is a senior news writer for SearchCompliance.com. Write to her at ltucci@techtargget.com.

Buyer Beware: The Complexities of Evaluating GRC Solutions

GRC is about more than governance, risk and compliance; it's about integration and streamlined management.

BY ED MOYLE



CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE



CHAPTER 2
A RISKY
APPROACH



CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

WHEN YOU GO shopping for a car, you likely have an inkling of what you want and shop at the appropriate dealer. If you want a truck, you're not going to shop at a Mini dealership; if you're after a sports car, you're not stopping by the Hummer dealer.

But what if every dealership advertised generic *vehicles*, and *vehicle* meant anything from cars to skateboards to locomotives? What if you couldn't tell who sold what because the product space was so big you couldn't differentiate one from the other? How would you start making a decision? This is the position buyers are in with governance, risk and compliance (GRC) products.

MASTERING THE SPIN CYCLE

GRC is a huge market with many vendors, each with its own GRC story.

These products are extraordinarily varied in the type of functionality they provide, the areas in which they excel and the aspects of the complete GRC picture where they have utility. And the way they're being sold? Well, saying it's difficult to tell which vendor does what is one whopper of an understatement. And it's not made any easier by the fact that there are multiple types of GRC: IT GRC, financial GRC, enterprise risk management, etc.

Vendors are spinning their products—everything from document management to technical control validation, risk analysis and identity management—to claim a slice of the GRC pie. IT and security managers with buying power are left confused and unsure about where to spend their GRC dollars. And at the end of the day, confusion is bad for everyone.

CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

CHAPTER 2
A RISKY
APPROACH

CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

For vendors, it means reduced adoption and a more difficult sales pitch. And for practitioners, it's an obstacle to a workmanlike approach to information security management and to getting internal traction for a GRC deployment. Confusion is, as is usually the case in IT, the enemy.

It isn't just the market—GRC as a product is huge as well. Breaking it

down, governance is the ability of management to ensure that activities are performed according to set, defined processes; risk management is about identifying and quantifying risk and making sure the organization operates within its risk tolerance; and compliance is the process by which the organization operates on the appropriate side of the law, industry

PROMISING PRODUCTS

Mapping GRC's claims to your company's requirements:

E-BUSINESS DRIVER

GRC "PROMISE"

Multiple overlapping regulations.

Regulatory framework construction allows multiple regulations to be mapped to one set of controls.

Demonstration of regulatory compliance to management/auditors.

Mapping of policy to controls and regulatory requirements allows you to keep track of compliance activities.

Difficulty managing numerous controls across multiple environments.

Monitoring tools for technical controls, ability to record which controls are implemented at what locations (and to satisfy what requirements).

Complexity of business makes risk evaluation difficult.

Ability to assign risk based on criticality of components and sensitivity of stored data. Ability to correlate changes in environment and controls to overall risk.

Burdensome tracking of policy exceptions including exception expiration.

Ability to track policy exceptions, owners of components in exception scope.

Inefficient, complicated or expensive security program management.

Ability to automate workflow for security program tasks such as exception approval, policy authorship and incidents.

↳
CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

↳
CHAPTER 2
A RISKY
APPROACH

↳
CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

regulation and policy.

Looking at it logically, vendors could make the argument that an identity management solution is IT GRC because it enforces governance, i.e., it helps ensure personnel follow the policies and procedures set down by management. Antivirus? Sure, why not? AV software that monitors its signature version and provides feedback about what machines don't have the software installed is policy enforcement at its finest. In fact, people could make the argument that every security product plays in the governance, risk and compliance space, to one degree or another—and they'd be correct.

But the point of GRC isn't just to govern, manage risk and comply; in fact, you're probably doing them all already. The point is instead how you do those three things. It's about transparency and integration—ultimately, by sharing a common vocabulary, these aspects of management can become more measurable, repeatable and, in the best case, efficient.

It's an evolution away from management processes that grew organically over time and a movement toward more streamlined, integrated and manageable processes that better serve the needs of your business. It's not about doing something new; it's about taking what you already do and refining it. And it doesn't take any particular product (or set of products) to get there.

In fact, many customers may not even realize they can get pretty far along in their GRC goals in-house without relying on a particular vendor. All it takes is an understanding of their requirements, a bit of organization and some planning.

People could make the argument that every security product plays in the GRC space, to one degree or another—and they'd be correct.

So in the interest of doing more with less, let's look at what you can do with tools you already have and try to move toward GRC nirvana. Once you know what you need and have started to chart out how far you can go without making a purchase, filling in the gaps with the products in the market becomes a totally different experience. Once you change your discussions with vendors from "What does your product do?" to "Does your product do this?" the process becomes much less stressful, less time consuming and, ultimately, easier to figure out.

DESIGN, THEN BUILD

The first step to implementing GRC is



PCI Compliance

across your virtual and physical infrastructures.

www.tripwire.com/pci

Tripwire helps you achieve and maintain PCI compliance - from your central systems out to your POS terminals. Automate PCI compliance by combining the required configuration control with Tripwire's enhanced file integrity monitoring. This enables immediate detection and response to security issues across your infrastructure, including virtual environments built with VMware ESX and Microsoft Hyper-V.

And because Tripwire generates a continuous audit trail, auditors can see proof of your PCI compliance across all virtual and physical infrastructures.

Hundreds of leading merchants in transaction-intensive environments rely on Tripwire® Enterprise to ensure the security of their customer's sensitive credit card data.

Check out our PCI Resource Center at:

www.tripwire.com/pci

tripwire[™]

↳
CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

↳
CHAPTER 2
A RISKY
APPROACH

↳
CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

to understand how you're currently running these aspects of your business, specifically how you'd like to improve and for what purpose. Figuring this out should be a group effort—what you're doing should have a broad impact on the whole organization and should be about integration—so this is not the time to create new silos in your organization. Reach out to all the stakeholders: IT, compliance, business, risk management, internal audit and counsel, and get them on board to help define requirements.

Some questions to ask in each aspect of GRC:

Governance: How are you currently organizing and publishing your policies and procedures? Do you even have policies and procedures? How are you enforcing them throughout the organization? Are you interested in just one particular set of policies and procedures, or is your interest more general—for example, are you just interested in IT or are you interested in business processes as well?

Risk management: What is your current process for identifying, classifying and treating risk? Are you using a formalized approach or an ad hoc one? Is that method quantitative or qualitative? Are you interested in just IT risk, or are you interested in other areas such as operational or financial risk?

Compliance: What is the extent of what you currently do for compliance? Are you currently using a compliance framework approach, or have all your efforts gone into targeting one or two specific regulations? Are you in a heavily regulated industry such as health care or financial services?

Coming to a quick and dirty understanding of where you are in each of these areas is a good first step and can give you valuable insight on

Reach out to all the stakeholders: IT, compliance, business, risk management, internal audit and counsel, and get them on board to help define requirements.

where you might see the most benefit from your investment. For example, if you're a health care provider and you've already spent more than a few dollars on risk assessment—i.e., to comply with the Health Insurance Portability and Accountability Act (HIPAA)—maybe risk management in your firm is in pretty good shape. Whereas if you're a small retailer, you might not have any formalized risk management in place—and so you

↳
CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

↳
CHAPTER 2
A RISKY
APPROACH

↳
CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

can benefit more from investment in this area. On the other hand, that same health care provider might have spent quite a bit of time and energy targeting HIPAA, and might not have a broad approach to compliance that covers other regulations that have developed since HIPAA was introduced. So maybe dollars are better spent expanding the compliance approach instead of concentrating on risk management.

Be honest with yourself about where you are and your maturity in these areas. If you're looking to move beyond a quick and dirty analysis and are looking for something a little bit more formal, take a look at the Open Compliance and Ethics Group's GRC Capability Model (the Red Book). This document provides a systematic (and highly detailed) outline for organizations looking to refine their overall GRC posture and seeking to implement these concepts within their organizations.

But at the end of the day, if it's a choice between setting the bar high and not making progress versus setting the bar low and moving forward, set the bar low. If you have the time, funding and patience for a thorough, formal and rigorous approach, so much the better. But if you don't, it's better to do something than nothing. The IT Policy Compliance Group in its 2008 annual report draws a direct parallel between IT GRC maturity and a firm's revenue; specifically, firms on

the highest end of the IT GRC maturity spectrum have 17 percent higher revenue than those at the lowest end. Meaning, it's in the best interest of your bottom line to do something.

REPACKAGE AND REPURPOSE

Once you have some idea of where you need help, determine whether there are tools in one area that you can expand to cover other areas. Remember again that the point of governance, risk and compliance is integration, so use this as an opportunity to find out what's working well and bring it into a broader fold. For example, maybe that tool that you're

If you're looking to move beyond a quick and dirty analysis, and are looking for something a little bit more formal, take a look at the Open Compliance and Ethics Group's GRC Capability Model (the Red Book).

using just for the internal audit crowd might be useful in other areas as well. Or maybe the IT tool that you're using to manage technical compliance could be repackaged for reporting

outside of just IT.

If you're a large organization, don't skimp on figuring out what you already have (chances are good that you already have something somewhere). This could include commer-

If you've already built a compliance framework based on standards such as the ISO 27000 series, NIST SP 800-53, COBIT or any other baseline, fold that process and documentation in as well.

cial tools that you've already purchased—for example, auditing-centric tools used to drive risk management, policy authorship and publication tools, management reporting tools or any number of other commercial products that have an impact in any of these categories. Technical tools that provide feedback on whether or not individual machines and user accounts are in line with defined policy are in scope as well. Take a thorough inventory of what you've already purchased so you don't buy something new with overlapping functionality (or so you can at least decide purposefully that you're

going to replicate functionality rather than discovering it after the fact), and so you can integrate what you already have into the broader scope of what you're trying to do.

Include also in-house tools that you may have developed. This could be an in-house tool with all the bells and whistles, but it could also be more humble tools such as the spreadsheets and reports provided for tasks such as reporting the status of audit items, tracking compliance with industry regulation or learning more about just about anything else that gathers or packages data about control effectiveness. If you've already built a compliance framework based on standards such as the ISO 27000 series, NIST SP 800-53, COBIT or any other baseline, fold that process and documentation in as well. If you haven't done that already, that's fine, too, but if you have, making sure that your approach reuses what you've already done will save time in the long run and avoid stepping on toes.

THINGS TO REMEMBER

After you've done these things, you'll probably realize a couple of things about your organization:

NO. 1: You're probably more interested in some areas of GRC versus others based on your particular needs.

NO. 2: You've probably already spent



CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE



CHAPTER 2
A RISKY
APPROACH



CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS

a dump truck full of money on tools and processes to help automate certain aspects of a complete GRC picture.

You may also realize that there are some areas where you haven't spent much in the way of time, effort or resources. Now you're ready to come up with a purchasing strategy for tools. And you should have a pretty clear idea about where a tool would be the most valuable.

Are you just interested in IT? Does your company have mostly manual processes in place? Maybe a turnkey technical solution is for you? When you shop around (and pilot those systems), you'll find out pretty rapidly that a vendor focused solely on risk management absent control validation is probably not the right choice.

Do you have fairly sophisticated technical processes and a heap of regulations to comply with (and not much in the way of compliance spending to date)? Maybe the vendor selling the technically focused solution isn't the right pick for your company.

Take a cue from the Oracle in *The Matrix* and "know thyself." Knowing what products you need before you invite the vendors in is the only way governance, risk and compliance will make any sense. ■

Ed Moyle is founding partner of consultancy Security Curve.

↳
CHAPTER 1
RISK MAN-
AGEMENT: THE
RIGHT BALANCE

↳
CHAPTER 2
A RISKY
APPROACH

↳
CHAPTER 3
BUYER BEWARE:
THE COMPLEXITIES
OF EVALUATING
GRC SOLUTIONS



GRC and Policy Management: Methods and Tools is produced by CIO/IT Strategy Media and Security Media, © 2009 by TechTarget.

MANAGING EDITOR CIO/IT STRATEGY MEDIA GROUP
Jacqueline Biscobing

ART DIRECTOR
Linda Koury

CONTRIBUTING WRITERS
Eric Holmquist and Ed Moyle

SENIOR NEWS WRITER CIO/IT STRATEGY MEDIA GROUP
Linda Tucci

EXECUTIVE EDITOR CIO/IT STRATEGY MEDIA GROUP
Scot Petersen

EDITORIAL DIRECTOR SECURITY MEDIA GROUP
Kelley Damore

SENIOR TECHNOLOGY EDITOR SECURITY MEDIA GROUP
Neil Roiter

FOR SALES INQUIRIES:
Stephanie Corby,
Senior Director of Product Management,
scorby@techtargget.com
(781) 657-1589

BUSINESS STAFF
SENIOR VICE PRESIDENT AND GROUP PUBLISHER
Andrew Briney

PUBLISHER, SALES
Jillian Coffin



- ▶ [IT Compliance Reporting: Delivering Continuous, Consistent IT Compliance](#)
- ▶ [nCircle Suite360: Automated Security & Compliance Auditing](#)



- ▶ [Stopping Data Leakage: Making the Most of Your Security Budget](#)



- ▶ [Beyond Payment Card Industry \(PCI\) Checklists: Securing Cardholder Data with Tripwire's Enhanced File Integrity Monitoring](#)
- ▶ [Configuration Control for Virtual and Physical Infrastructures: How the Visible Ops Approach Offers Solutions to the Problem of Unplanned Work](#)
- ▶ [File Integrity Monitoring: Secure Your Virtual and Physical IT Environments](#)