CHAPTER 1
Metrics a Must for Risk Management

CHAPTER 2
Integrated GRC Needs a Holistic Approach

CHAPTER 3
Four Considerations for Your ERM Strategy

CHAPTER 4
Managing Social Media? Prepare for the Worst

Safeguarding Against a World of Threats

An enterprise risk management strategy is critical to companies looking to understand threats and minimize their impact.

Metrics a Must for Risk Management

CHAPTER 1
Metrics a Must for Risk Management

CHAPTER 2
Integrated GRC Needs a Holistic Approach

CHAPTER 3
Four Considerations for Your ERM Strategy

CHAPTER 4
Managing Social Media? Prepare for the Worst

Analyzing trends in your current compliance initiatives can help you assess future risk management needs.

BY KEVIN BEAVER

PERHAPS YOU'VE HEARD the saying "what gets measured gets done." This is business wisdom at its finest. With regards to IT, however, what if you feel like you can't measure certain things? After all, calculating information risks, ROI and so on can be difficult. But it's probably because you haven't looked at it deeply enough: The reality is, if you step back and look at the big picture, you can indeed measure the critical areas of IT. It's just a matter of metrics.

Metrics can drastically improve your information risk management and compliance initiatives, but you must take the initiative to go down that path. In *Keep the Joint Running: A Manifesto for 21st Century Information Technology*, Bob Lewis wrote, "Bad metrics are worse than no metrics: If you have no metrics, you're ignorant and know it. Bad metrics, in contrast, give either the wrong answer to the right question or answer the wrong question." I agree.

If you have some semblance of metrics—no matter how much they need to be tweaked—you're at least going down the right path. Sadly, many organizations just approach each year with a sequence of events that goes something like this: scan, audit, plug the holes, scan, audit, plug the holes. It's functional, but it's probably not the best way to go about managing risks and compliance. Like most areas of any business, there's always room for improvement.

The reality is that risk management metrics can be tricky, if not downright scary. But they don't have to be if you follow the proven approach. You must first define what "good" information risk management and compliance means in your business. Perhaps it's no breaches? Maybe it's not getting any dings on your quarterly scans or annual audit reports? One security breach or compliance gap doesn't necessarily mean failure. No security

CHAPTER 1
Metrics a Must for Risk Management

CHAPTER 2
Integrated GRC Needs a Holistic Approach

CHAPTER 3
Four Considerations for Your ERM Strategy

CHAPTER 4
Managing Social Media? Prepare for the Worst

breaches or gaps doesn't necessarily mean success. The key is to look at trends. How effective are your compliance and security measures? Are they efficient enough, or is there still room for improvement? Only you and your fellow business managers can define what matters and ultimately what's considered a "success" for the business.

Digging in deeper, you need appropriate controls based on the level of risk. Not everything counts the same. You're likely already taking this approach as many regulations are risk-based, including the Health Insurance Portability and Accountability and Gramm-Leach-Bliley acts. Part of the initial legwork has already been done, but you have to dig much deeper. Some questions you need to answer include:

- What do you have of value?
- How is it at risk?
- How are these risks changing over time?
- What is it costing you to manage these risks?
- How much can you afford to lose?
- How successful are your controls?
- Do you have the proper insight into what's taking place in your environment?
- What else can be automated or outsourced to further reduce your risks and improve overall compliance and security?

Think about these areas across all parts of the risk management spectrum, from your information systems infrastructure and data to your policies and people. Everything matters, and you better make sure you're looking at everything—not just what some regulation says. Information risk management is about managing all of your risks across the board.

> Risk management metrics must be periodically and consistently measured; otherwise, you have bad data—and you can't run a business on bad data.

Be aware that you don't want to go at this alone. This is going to require getting others involved—especially executive management. Information risk management and metrics aren't something that one person should manage.

Risk management metrics must be periodically and consistently measured; otherwise, you have bad data—and you can't run a business on bad data. A snapshot-in-time vulnerability assessment or an annual compliance audit aren't enough. The process for gathering risk management metrics data needs to be automated wherever possible. I see lots of organizations

CHAPTER 1
Metrics a Must for Risk Management

CHAPTER 2
Integrated GRC Needs a Holistic Approach

CHAPTER 3
Four Considerations for Your ERM Strategy

CHAPTER 4
Managing Social Media? Prepare for the Worst

that have fancy IT and security monitoring and maintenance systems, but the people in charge are not using them anywhere near their potential.

> Metrics are like goals. They need to be specific, measurable and have a timeline, and someone needs to be held accountable.

Many others make the choice not to invest in the right tools and, thus, the lack of visibility and insight continues.

The bottom line is that metrics are like goals. They need to be specific, measurable and have a timeline, and someone somewhere along the line needs to be held accountable. Otherwise, they're mere wishes that lead to delusions that lead to compliance gaps and business risks that you're probably not willing or prepared to take on.

Why not establish a set of risk management metrics and do it the right way from the get-go? Don't focus on statistics alone. Rather, focus on understanding what's really going on with your information systems. By doing so, you'll be able to get a better handle on what works and what doesn't. Adaptability and continual improvement are must-haves in the world we work in and must eventually become second nature to your business. ■

Kevin Beaver is an information security consultant and expert witness, as well as a seminar leader and keynote speaker at Atlanta-based Principle Logic LLC. Write to him at editor@searchcompliance.com.

CHAPTER 1
Metrics a Must for Risk Management

CHAPTER 2
Integrated GRC Needs a Holistic Approach

CHAPTER 3
Four Considerations for Your ERM Strategy

CHAPTER 4
Managing Social Media? Prepare for the Worst

Integrated GRC Needs a Holistic Approach

A cohesive governance, risk and compliance framework can make your compliance strategy more effective. Here's how.

BY JOHN WEATHINGTON

GOVERNANCE, RISK AND compliance should not be seen as separate concerns, but as parts of a holistic or cohesive GRC framework. As with anything, concepts are important, but without a tangible GRC technology architecture to bring the concepts into reality, the outer bounds of their usefulness won't go beyond cocktail-party conversation.

Prominent on President Barack Obama's agenda when campaigning for, then subsequently stepping into, the White House was transparency. *Transparency* has always been obvious to those of us in regulatory compliance; however, the 2008 campaign made it a household word. On Jan. 21, 2009, our newly inaugurated president issued a memorandum on transparency and open government, wherein he directed the country's chief technology officer (CTO) to coordinate the development of an Open Government Directive designed to accomplish his goals of transparency, public participation and collaboration.

> Architecting a system of transparency with the right technology is paramount to your integrated governance, risk and compliance solutions.

Whether you agree with President Obama's policy or not, it's hard to disagree with the importance of transparency. What I'd like to highlight here is that he put the CTO in charge of this effort, which drives home the role he feels technology plays in the overall solution. I completely agree.

Architecting a system of transparency with the right technology is

CHAPTER 1
Metrics a Must for Risk Management

CHAPTER 2
Integrated GRC Needs a Holistic Approach

CHAPTER 3
Four Considerations for Your ERM Strategy

CHAPTER 4
Managing Social Media? Prepare for the Worst

paramount to your integrated governance, risk and compliance solutions. I'll give you a starting point here with some ideas to consider; however, I exhort you to experiment. By keeping the basic concepts and principles in mind, your compliance system can become very effective at accomplishing not only your compliance objectives, but also your strategic goals.

HOLISTIC GRC FRAMEWORKS: A QUICK REVIEW

Let's quickly review these concepts of an integrated system, and then we'll explore some architectural considerations. Governance is concerned with the policies and controls that an organization has in place to ensure that its missions and goals are being accomplished. Risks are uncertain events that can derail the organization's success (i.e., interfere with governance objectives) and expose your organization to violations of outside concern. Compliance involves processes and controls to make sure these risks either don't show up or don't adversely affect the organization, in addition to proving that these processes are being followed and these controls are effective.

The more integrated your governance, risk and compliance solutions, the more effective they will be. You could design silos with separate concerns, but the real power is in the relationships.

That said, each component should maintain its autonomy of purpose. Do not integrate to the point where you cannot distinguish one subsystem from another. Just like quoting, order management, invoicing and collection systems all fit together to form a holistic quote-to-collect system with identifying subsystems, you'll want your governance, risk and compliance subsystems to fold nicely together but not purée.

> The more integrated your governance, risk and compliance solutions, the more effective they will be. You could design silos with separate concerns, but the real power is in the relationships.

BRING GRC SOLUTIONS TOGETHER

To show you how this works, I'd like to use the example of organizational diversity. We can start anywhere, but I usually like to start at the top, with governance. When I work with leaders on diversity issues, it's for one of any number of reasons, but good leaders recognize that building diversity within the organization is a very strategic

CHAPTER 1
Metrics a Must for Risk Management

CHAPTER 2
Integrated GRC Needs a Holistic Approach

CHAPTER 3
Four Considerations for Your ERM Strategy

CHAPTER 4
Managing Social Media? Prepare for the Worst

move. Cultivating a hodgepodge of talent from diverse backgrounds and cultures puts the organization at a distinct strategic advantage.

Consider a young, midsized company that's in hypergrowth, both in revenue and head count. Innovation is valued and used as a competitive advantage. Strategically, the company has determined that its driving force for the next three years will continue to be innovation, building on its current strength and increasing its competitive advantage. To do this, the company will double head count, with a constraint that the resultant organization be fully diverse.

To start, install your subsystem of governance. Your strategic goal is increased innovation, so you manufacture an innovation index and use it as your key performance indicator.

MEASURE RESULTS WITH YOUR GRC SOLUTIONS

The assumption here is that a more diverse group is more innovative, so you need to track this assumption (and others). You'll now create policies to make sure innovation is accomplished and, consequently, a policy management system is established. For instance, you could create a policy that, out of 20 diversity classes, no one class should represent more than 7% of the total talent pool. Periodically, you will check your policy statements with objective data to make sure things are as they should be. The identification and tracking of these objective data points are all part of your policy management system.

> Install your risk subsystem by asking what could go wrong—brainstorm with your team. Characterize each risk with a probability, degree of impact, ability to detect and possible causes.

You should then build a set of plans and procedures that will ensure that your policy is maintained, and a system to make sure they're being followed. Next, install your risk subsystem by asking what could go wrong—brainstorm with your team to uncover all of the risks you can imagine. Don't be naive—this should be a very long list. Characterize each risk with a probability, degree of impact, ability to detect and possible causes. Track all of this data in your risk subsystem and link it to your governance subsystem, with a bridge between each policy or procedure and all of the risks that could interfere with its successful execution.

Finally, to build your compliance subsystem, you will now do a couple

CHAPTER 1
Metrics a Must for Risk Management

CHAPTER 2
Integrated GRC Needs a Holistic Approach

CHAPTER 3
Four Considerations for Your ERM Strategy

CHAPTER 4
Managing Social Media? Prepare for the Worst

of things. First, fortify the plans and procedures system you created for your governance subsystem by exploring what procedures you can put in place to mitigate the risks you uncovered when building your risk subsystem. Second, you'll look at outside concerns, like federal laws established by the Equal Employment Opportunity Commission, to make sure your goals in diversity are in alignment with them. From these laws, you'll uncover additional risks that you might not have considered, which will reinforce your risk subsystem and require the further creation of policies. Finally, to finish your compliance subsystem, you'll create a system to collect, track and index evidence that will prove your innocence in an audit.

I hope this quick example shows you how governance, risk and compliance solutions can fit together to accomplish your strategic goals and keep you out of trouble. For governance subsystems, which ensure your strategic success, consider ways to measure your key performance indicators and track your assumptions, policies and procedures. For risk subsystems, catalog and track all the things that could go wrong with your policies, and mitigate these risks with controls in your compliance subsystem. Finally, reinforce everything by considering the regulations and standards from outside concerns, and build a compliance subsystem that proves you're doing all the right things.

> For risk subsystems, catalog and track all the things that could go wrong with your policies, and mitigate these risks with controls in your compliance subsystem.

If you have silos now (i.e., a separate compliance and risk system), look at ways to combine them using the principles presented here. If you're just beginning to construct a GRC system, I hope this article has given you some insights on how to get the most from your system by focusing on the integration points, not just the individual components. ■

John Weathington is president and CEO at Excellent Management Systems Inc., a San Francisco-based management consultancy. Write to him at editor@searchcompliance.com.

Four Considerations for Your ERM Strategy

CHAPTER 1
Metrics a Must for Risk Management

CHAPTER 2
Integrated GRC Needs a Holistic Approach

CHAPTER 3
Four Considerations for Your ERM Strategy

CHAPTER 4
Managing Social Media? Prepare for the Worst

An effective enterprise risk management strategy accounts for more than just security and continuity. Discover what you may be missing.

BY SCOTT LOWE

WHEN PEOPLE ASSOCIATE the word *risk* with IT, the first thing that often comes to mind is some hacker breaking into the corporate network to steal sensitive customer information for resale on the black market. Or they envision a lost or stolen laptop containing millions of transaction records, credit card numbers and so forth. After all, these kinds of events, when they occur, are often big news and are highly visible.

Such incidents are only a small part of what should be mitigated through the use of a comprehensive risk management strategy. However, just like any other business initiative, a risk management strategy has to be a business priority, and it's entirely possible that some organizations will pick and choose which components to include in an overall risk management plan. It simply comes down to what makes sense for a particular company. Here are four aspects to consider as you define your risk management strategy.

DON'T RUN THE RISK OF IGNORING BACKUPS

Regardless of the organization, taking good backups must be a universal part of an overall risk management strategy, although the exact method may vary. Without some method for backing up critical business information, recovery is impossible. Some statistics indicate that 90% of companies that suffer major data loss go out of business within two years.

Given the breadth and depth of choice when it comes to backup software, this is one risk management item there is no reason or excuse to overlook or ignore.

Taking a backup, however, isn't nearly enough. Organizations need to routinely test backup quality and com-

CHAPTER 1
Metrics a Must for Risk Management

CHAPTER 2
Integrated GRC Needs a Holistic Approach

CHAPTER 3
Four Considerations for Your ERM Strategy

CHAPTER 4
Managing Social Media? Prepare for the Worst

pleteness. Backups can be notoriously fickle, and it's amazing just how bad they can be. I worked in an organization once that had previously fired its entire IT department after discovering that there were no good backups of the financial system for six months.

> Data can be accessed from all kinds of locations, and securing that data can be a pretty significant task. Employees can store massive amounts of data on portable devices and then lose said devices or have them stolen.

The following items should be included in any risk management policy related to backup:

- Backup frequency, type (full or differential) and retention for each type of data being protected.
- Short-term and long-term backup and recovery objectives.
- Backup process and quality testing frequency and procedures.
- Backup location—this should be off-site.

DATA AND NETWORK SECURITY

Data can be accessed from all kinds of locations, and securing that data can be a pretty significant task. Employees can unwittingly (or wittingly) store massive amounts of data on portable devices and then lose said devices or have them stolen. This is one area of a risk management plan in which the argument of security vs. usability needs to be made. How much user flexibility are you willing to compromise to protect the integrity of your data?

Data security consists of both organizational policies and technological measures implemented together. The following should be included in your risk management processes:

- Access controls for sensitive data, such as personally identifiable customer information.
- Policies—both organizational and technological—controlling on which devices data can be saved. For example, should users be allowed to save information to removable devices such as flash drives?
- Policies and measures for encrypting information on mobile devices, including full disk and mobile storage device encryption.

As part of this process, don't ignore items such as your organization's password policies. Password policies should include password expiration and complexity, as well as thresholds

CHAPTER 1 Metrics a Must for Risk Management

CHAPTER 2 Integrated GRC Needs a Holistic Approach

CHAPTER 3 Four Considerations for Your ERM Strategy

CHAPTER 4 Managing Social Media? Prepare for the Worst

at which a user's account becomes disabled.

From a mobility perspective, consider newer technologies, such as virtual desktop infrastructure, that keep information inside the data center at all times. Further, test your network security through vulnerability assessments performed from time to time.

DON'T FORGET TO ADDRESS PHYSICAL SECURITY

Physical security is an integral part of a risk management strategy and includes a number of components to consider:

- Controlling access to critical infrastructure, such as the data center and intermediary communications hubs.
- Maintaining appropriate environmental control and monitoring at the location of critical infrastructure. For example, does the data center have a fire-suppression system that can preserve both equipment and human life? Does the data center have monitoring systems that ensure that temperature and humidity remain inside specified parameters?

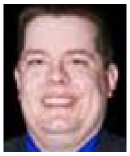
Physical security controls also need to be present in the other components of a risk management strategy, including access to tapes or other backups and control of mobile devices.

BUSINESS CONTINUITY AND HIGH AVAILABILITY

A fire, natural disaster or other major event can spell catastrophe for an organization and its survival. In order to ensure that it's business as usual as much as possible, many organizations choose to develop comprehensive business continuity plans that define, in detail, what steps are taken to regain or remain in operation. With technology playing a major role in the operation of many businesses, ensuring that IT assets remain available is high on the business continuity/availability list.

High availability is often part of an overall risk management strategy and can entail such activities as building clustered services, implementing RAID sets on storage devices or moving to a fully redundant architecture based on VMware, for example. It can also mean the development of a fully redundant standby data center that can assume control in the event of the loss of service in a main data center.

There are numerous examples of high-availability strategies found in software today, including the aforementioned clustered services and VMware High Availability. You can also look at features like Microsoft Exchange 2010's Database Availability Groups, and technologies like it. ■



Scott Lowe is vice president and CIO at Westminster College. Write to him at editor@searchcompliance.com.

Managing Social Media? Prepare for the Worst

CHAPTER 1 Metrics a Must for Risk Management

CHAPTER 2 Integrated GRC Needs a Holistic Approach

CHAPTER 3 Four Considerations for Your ERM Strategy

CHAPTER 4 Managing Social Media? Prepare for the Worst

Computer forensics is perceived as a science rarely used by compliance officers, but that's just not the case.

BY KEVIN BEAVER

SOCIAL MEDIA CAN be used as a tool or a weapon, and it's important to be aware of the powers and the dangers inherent to it. I will probably let my young son tweet before I let him use my chainsaw, but the warning lecture will be no less graphic.

We may have already seen the first—but far from the last—high-profile case of professional suicide by Twitter. Rep. Anthony Weiner (D-N.Y.) made several technical and tactical errors with social media last spring—including accidentally displaying lewd photos to the world via Twitter—that contributed to his resignation. In a similar case that received less coverage in the U.S., Canadian political candidate George Lepp tried to explain a questionable photograph by claiming it was taken inadvertently when his BlackBerry was in camera mode in his front pocket, and then sent out by an unknown person. This impossible account led to a very public and embarrassing search for plausible alternative explanations.

Both are cases of easily avoidable injury, so perhaps it's time to consider a few social media risk management guidelines to stem the tide of such needless incidents.

Social media provides a set of tools. Results will largely depend on understanding how the technology works and how others may exploit it. It's easy to go too far in constraining the use of social media, which deprives users of many of its benefits. For example, in my town, the board of education enacted a social media risk management policy for teachers and administrators. It sparked a backlash, as the policy explicitly forbade a variety of generally innocuous activities in an attempt to prevent some serious problems; however, those were already covered by existing policies and common sense. In other words, it ruled out the possibility of positive interactions between teachers and students to avoid potentially damag-

CHAPTER 1 Metrics a Must for Risk Management

CHAPTER 2 Integrated GRC Needs a Holistic Approach

CHAPTER 3 Four Considerations for Your ERM Strategy

CHAPTER 4 Managing Social Media? Prepare for the Worst

ing ones.

A balance between draconian measures and anarchy surrounding social media risk management is required. With that in mind, here are four assumptions that provide a starting point for social media risk policies for individuals and enterprises.

Assume that you will make mistakes. Forgetting to put a *d* at the beginning of a direct message on Twitter—one that can be seen by only an individual recipient—is basic, but everyone I know has a personal story of (t)error on this one. In my own experience, it has been known to happen when I use TweetDeck on my iPhone from a train without bothering to put on my glasses. Committing this common error started the public unraveling of Weiner.

Policy implication: Nothing that could conceivably damage the safety, security or reputation of you or your enterprise should be transmitted by direct message. This means that messages must be classified according to the potential risk of unrestricted distribution. Any item that has a high risk should be transmitted using encryption, or at the very least only to individuals known to follow these policies themselves.

Any item that has a high risk should be transmitted using encryption or, at the very least, transmitted only to individuals known to follow these policies themselves.

Assume that others will make mistakes. Countless cases of individuals sending emails inadvertently using "Reply All" should have taught us that nobody can be counted on to be error-free. The analogs with social media include responding to someone on a (public) Facebook wall instead of sending a private message, or having the recipient of a direct message respond with a public message. It happens. Plan for it.

Policy implication: Make it difficult for others to expose your secrets through carelessness. Do not use social media for antisocial messages.

Assume that someone is out to get you. Paranoid? Perhaps, but who in business or politics has nobody who would delight in his downfall? Weiner may have sent pictures to individuals who appeared willing to receive them, but his enemies soon convinced recipients to share the pictures for political purposes.

Policy implication: Recipients of sensitive material must be vetted and classified. In Facebook, start by limiting access to friends rather than

CHAPTER 1
Metrics a Must for Risk Management

CHAPTER 2
Integrated GRC Needs a Holistic Approach

CHAPTER 3
Four Considerations for Your ERM Strategy

CHAPTER 4
Managing Social Media? Prepare for the Worst

friends of friends (or limit Facebook use to purely personal topics). For Twitter, use the same criteria you would for a nonsecure telephone line.

> Personal mobile devices do occasionally fall into the wrong hands.

Assume that your phone or laptop will fall into the wrong hands. While sometimes it's only a lame excuse, personal mobile devices do occasionally fall into the wrong hands. I recently received a text from a colleague I know well, and the content was inappropriate. The next day I learned that her phone had been "borrowed" by a prankster.

Policy implication: For most of us, the value of our reputation and data far outweighs the replacement value of a device. Always use password protection, selectively use encryption, and have a remote wipe contingency plan for all digital devices that could be used to send out messages "from you." Passwords for social media accounts should be as strong and as secret as those for financial accounts. ■

Adrian Bowles is vice president and principal analyst at Constellation Research Inc. and founder of SIG411 LLC, a sustainability consulting firm in Westport, Conn. Write to him at editor@searchcompliance.com.

SearchCompliance.com

Safeguarding Against a World of Threats
is produced by CIO/IT Strategy Media,
© 2011 by TechTarget.

Jacqueline Biscobing
Managing Editor

Rachel Lebeaux
Assistant Managing Editor

Linda Koury
Director of Online Design

Scot Petersen
Editorial Director

Chris Gonsalves
Executive Editor

Ben Cole
Associate Editor

Kevin Beaver
Adrian Bowles
Scott Lowe
John Weathington
Contributing Writers

FOR SALES INQUIRIES

Corey Strader
Director of Product Management
cstrader@techtarget.com
(617) 431-9621