contents

Strategies for Understanding GRC

2 GRC Complexity
8 Compliance Intersection
18 Federated GRC
22 Governance Frameworks
26 Resources

Understanding GRC

Governance, risk and compliance frameworks, tools, and strategies are essential to the success of today's corporate information security programs.

BY INFORMATION SECURITY AND SEARCHSECURITY.COM

Buyer Beware: The Complexities of Evaluating GRC

BY ED MOYLE

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

Remember the last time you went shopping for a car? You likely had an inkling of what type of car you wanted, and shopped at the appropriate showroom. If you prefer trucks, you're not shopping at a Mini dealership, and if you're after a high-end 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 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 their own GRC story. These products are extraordinarily varied in the type of functionality they provide, the area(s) 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.

These products are extraordinarily varied in the type of functionality they provide, the area(s) in which they excel, and the aspects of the complete GRC picture where they have utility.

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. 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 an obstacle to getting internal traction for a GRC deployment. Confusion is, as is usually the case in IT, the enemy.

Not only the market, but GRC as a product is huge. 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 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, someone could make the argument that every security product plays in the GRC space to one degree or another–and they'd be correct.

'PROMISING' PRODUCTS

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

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 what 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

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 that 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.

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 to understand how you're currently running these aspects of your business and specifically how you'd like to improve, and for what purpose. And 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. 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 that

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

they're followed throughout the organization? Are you interested in just one particular set of polices 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 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 HIPAA security rule), 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 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 (OCEG) "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.

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 (OCEG) "GRC Capability Model" (the Red Book).

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 (ITPC) 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 GRC 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 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 commercial 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 that you can at least decide purposefully that you're going to replicate functionality rather than discovering it after the fact), and so that 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

Take a thorough inventory of what you've already purchased so you don't buy something new with overlapping functionality.

spreadsheets and reports that are currently provided for tasks such as reporting the status of audit items, tracking compliance with industry regulation, or just about anything else that gathers or packages data about control effectiveness. If you've already built a compliance framework based on a standards such 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 few things about your organization. No. 1, you're probably more interested in some areas of GRC versus others based on your particular needs, and No. 2, you've probably already spent 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? Do you have mostly manual processes currently 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 but 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.

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 GRC will make any sense. *

Ed Moyle is founding partner of consultancy Security Curve.

If you've already built a compliance framework based on a standards such the ISO 27k series, NIST SP 800-53, COBIT, or any other baseline, fold that process and documentation in as well.

Push-button Compliance

BY MICHAEL S. MIMOSO

Companies are finding innovative, all-encompassing ways to satisfy multiple regulations.

If you're responsible for security, risk management and/or compliance for a global pharmaceutical distributor, a large data provider or a small municipality, you're at the cross-section of federal and industry regulatory compliance.

Regulation bombards you from every direction. Failure to meet federal and state mandates such as Sarbanes-Oxley and state data breach notification acts threatens the reputation of your corporate brand and the personal freedom of your executive officers. Falling short on industry requirements such as HIPAA, PCI, the Fair Credit Reporting Act or even state law enforcement accreditation puts in jeopardy your company's ability to do business as well as your customers' personally identifiable information.

As an information security and risk professional, you've been thrust during the last half-decade into the crosshairs of an increasingly regulated business environment. Frameworks, audits, automation and GRC are the fabric of your being.

Redundancy cannot be.

"What you don't want to do is implement or test the same control three, four, five times over," says Marc Othersen, senior analyst in the security and risk management practice at Forrester Research.

So how are businesses managing multiple regulations without a massive duplication of efforts? Is there a catch-all framework that satisfies all the overlap?

Three enterprises servicing three different markets are building their version of a compliance "easy button," drawing on a multi-

As an information security and risk professional, you've been thrust during the last half-decade into the crosshairs of an increasingly regulated business environment.

tude of resources to create a repeatable set of processes that would satisfy the grumpiest auditor.

MENDED SOX LEADS WAY

"It's definitely our approach to create a strategy that will be all-encompassing," says John Sapp, senior manager, IT governance, risk and compliance at McKesson Corp., the country's largest pharmaceutical distributor. "Whether it's regulatory compliance or compliance with our own internal policies, it's basically building that big picture first, and then deciding how we're going to approach it and ensure that we're doing it in a way that allows us to be really integrated across-enterprise and move away from the siloed approach that we so often see."

McKesson, with $101.7 billion in revenue in FY2008, has a mature Sarbanes-Oxley compliance program, and this is the model Sapp and his team are following to build a one-stop enterprise-wide compliance program.

Sapp, who has a development and project management background, says his organization isn't unlike much of the Fortune 500 in wanting to develop a set of repeatable processes to address compliance. He has taken steps to identify and understand McKesson's IT environment, map out and automate the testing of controls, assess and report on risk and increase the overall maturity of the organization's risk and compliance program. Right now, he says, McKesson is in an ad-hoc state, moving toward repeatable, and eventually standardized and optimized, processes.

"In three years, I would expect that we are

MANAGEMENT

What's in a Title?

IT GRC may be suffering from some hype overload, but McKesson's John Sapp doesn't see it that way. In fact, he buys into the concept so much, he baked it into his title: senior manager, IT governance, risk and compliance.

Sapp is one of the first to hold a senior GRC title, though Colgate-Palmolive has a manager in a similar position, and Apple Computer is advertising to fill a similar role.

Sapp formerly was senior consultant for risk services at McKesson, but as the company dedicated more resources to GRC and its overall compliance initiatives, it needed a senior manager in the role.

"Working with our VP of IT risk management, I wrote the job description and title two months ago in response to the GRC movement," Sapp says. "We found we wanted to create a single point of contact for all compliance and risk management activities, and be able to deliver some level of reporting—the governance piece—to be able to monitor the entire program across the enterprise."

–MICHAEL S. MIMOSO

at a standardized state," Sapp says. "That, for me, has us where we have a set of standards, processes and controls that are applied across the enterprise universally and consistently, moving toward optimized where we really almost get to a plug-and-play environment where regardless of who we acquire, we can plug them in, or if we choose to sell off an entity, it makes it an easy process for us."

Formerly, as McKesson's senior consultant for risk services *(see "What's in a Title?," see p. 9)*, Sapp was business unit SOX coordinator in charge of the IT controls for the SOX program. Upon moving to his broader role, he quickly discovered how McKesson's numerous acquisitions had created a situation where the company operated in silos, with precious little in the way of standardized processes or a lifecycle approach for addressing regulatory mandates. His goals quickly became clear: overcome the siloed approach and build a program that will allow him to drive corporate performance through these activities.

McKesson's SOX program leverages the ISO 27001 standard for information security management and the COBIT framework for IT management and metrics.

Sapp says his organization has deployed Brabeion IT GRC suite to manage policies and map multiple regulations, such as PCI and HIPAA, to control frameworks. But he believes a collaboration of tools will ultimately meet McKesson's needs to get to integrated GRC and he is evaluating several other tools such as asset management and configuration management databases (CMDB).

SOX, PCI and HIPAA are McKesson's three largest compliance issues, and the company's SAP environment, which it uses for its financials, is the primary area of concern.

"We found many parallels where one piece of ISO will satisfy parts of each one of those regulations," Sapp says. Access controls, for example, are codicils of each of those regulations. "ISO allows us to map across that and ensure by meeting that one ISO objective, I can test once, and certify many [times]. If I'm using the same access control process across each one, then I can reduce the amount of testing I do. That's what I've been able to do with our SOX program. I can drastically reduce the amount of time we spend in audits because we have improved our process so much. We're getting through audits in what I would

"I can drastically reduce the amount of time we spend in audits because we have improved our process so much. We're getting through audits in what I would call record time and within our budget."

John Sapp,
senior manager,
IT governance,
risk and compliance,
McKesson Corp

call record time and within our budget."

Sapp's current evaluation of GRC tools, he hopes, will further put out to pasture the tedious, laborious manual processes in place for collecting data from business units, testing and mapping controls to particular regulations. With 200-plus controls applicable to the SOX program, Sapp says that was his first target for automation with the Brabeion tool.

"We looked to an automated tool to help us be able to test the controls, attach the evidence and keep the user from going to the next step," he says. "I had one user tell me we've improved the quality of life here. We actually used SharePoint prior to automation, but the workload isn't there that you get in these tools."

Sapp says the GRC tools he's seen do a fine job of defining the assets and entities of an organization. He says they are solid for analyzing workflow and creating dependencies; this kind of intelligence can be applied outside of GRC as well. He adds that the tools are sound for collecting asset information (e.g., identifying unsupported or expiring versions of software), which helps in a risk assessment. Finally, he says the dashboard facilities are a strong means of providing a risk picture to the C-level.

In contrast, he says some tools try to do too much, and don't do very much very well. Products billed as turnkey, full-enterprise GRC programs sometimes suffer from poor workflow because of misguided focus. "Vendors sell hard on the tool rather than getting you to step back and look at process and strategy," Sapp says. "They don't think process and strategy first; they throw this toolset at you and say this will solve all your problems."

Forrester's Othersen says the tools at their core address compliance well, mapping sources, automating manual tests and providing solid reporting. Where they fail is in not linking IT risk to business risk.

"They don't have a business perspective in their risk engines," Othersen says. "All of them are IT focused, yet most risk happens in the line of business. If you lose credit card numbers, the line of business pays, not IT. Translating IT control failures into business risks is one of the biggest failings of those packages."

He adds that they don't address governance, either. "It's up to you as a CIO or security manager to use the tool to collect and analyze data on your own."

> "Vendors sell hard on the tool rather than getting you to step back and look at process and strategy."
>
> John Sapp, senior manager, IT governance, risk and compliance, McKesson Corp

A FERM TOUCH

The vagaries of regulatory compliance have left many information security professionals on an island. Your interpretation of regulation is often as important as the controls you implement to meet the intent and rigor of a federal law or industry mandate.

Isabelle Theisen, chief security officer for First Advantage Corp., deals with these vagaries with a homegrown concoction of established frameworks, processes and automated tools that implement not only a solid compliance program, but sound business practices *(see "Consistency Counts," p. 16)*.

"Business sees anything having to do with compliance as a necessary evil; they need it because they're being told they need it," Theisen says. "I'm trying to turn that around and say, 'No, you can also use IT governance, self compliance, business operations compliance and security to actually be a market differentiator against your competitors. You can turn it around and use it as a way of doing a better job against your competitors."

First Advantage is a data provider, servicing car dealers, mortgage services and employers with credit reports, background checks, skills assessments and more. The California-based company is subject to Sarbanes-Oxley, the Federal Credit Report Act, Gramm-Leach-Bliley, PCI and state data breach notification laws and privacy laws. Some of the regulations' requirements overlap, and prescriptive advice is minimal.

In response, Theisen architected what she calls the FERM (First Advantage Enterprise Risk Management) program to identify controls to cover as many regulations as possible. The framework is a blend of COBIT, ISO and NIST recommendations and a mix of manual processes to identify risk and controls and ultimately feed them into a GRC tool from ControlPath, which the company purchased 18 months ago.

"We implemented the tool across business units to perform assessment, identification, testing and remediation work to ensure we meet compliance for all of our business units," she says.

Theisen compared the manual processes in place prior to automation to typical audit work—lots of face-to-face interviews, surveys and questionnaires to determine what was in place in the different business units and inventory security, risk management, IT governance and other regulatory processes.

> Your interpretation of regulation is often as important as the controls you implement to meet the intent and rigor of a federal law or industry mandate.
>
> Isabelle Theisen, chief security officer, First Advantage Corp.,

This information was kept in a spreadsheet—not practical, Theisen says. Now it is updated into the ControlPath tool.

"I would always recommend an automated tool," Theisen says. "You do have to have a repository of that information, even if you build an easy Access database. Otherwise, you're going to ask the same questions every year to the businesses. How would you build a baseline? It would be a nightmare to manage your compliance levels manually."

Automation also helps with trending and tracking of progress against control objectives.

Identification is the first of four deployment phases of the FERM process. Inventory such as service offerings and business unit assets are gathered and uploaded to the tool.

Assessment is the next phase. Threats, vulnerabilities and risk that could impact a particular service offering are assessed. Business impact analysis, data classification and threat modeling are done against every application that applies to a service offering in a business unit. "Because we do a data classification, we can focus only on high-risk applications for a service offering," Theisen says. "Business management has been extremely supportive because they know we are focusing on what is critical to them—high-risk applications within their service offering—and we don't have to do everything."

Those two phases are the most time consuming, she says, but are absolutely necessary.

The third phase is testing. Having established what the high-risk issues are, Theisen's group can focus on what is critical to a business unit. Application and infrastructure assessments are conducted prior to a controls analysis questionnaire. The questionnaire is tailored to the service offering in question, Theisen says. ControlPath builds a master controls library mapped to all the controls relevant to First Advantage, enabling it to build customized questionnaires for each business unit.

"It's where automation matters," she says.

Remediation is the final phase. Based on the results of testing, Theisen has a list of remediation items prioritized based on risk—all flowing from the organization's business impact analysis and data classification.

Theisen says a major challenge involves keeping up with the fluid changes in regulations where very little automation exists on the front end to gather data. Often organiza-

"Business management has been extremely supportive because they know we are focusing on what is critical to them—high-risk applications within their service offering—and we don't have to do everything."

Isabelle Theisen, chief security officer, First Advantage Corp.,

tions are forced to wait for vendors to update their control libraries, or do it manually.

Another challenge is the narrow focus on compliance versus doing what is right for the business by implementing sound business practices to manage data.

"I try to stay away from talking about regulations," Theisen says. "This is about sound business practices."

ITIL LEADS WAY

Public agencies may be exempt from the whims of Wall Street, but that doesn't ease the regulatory demands placed upon them. Their compliance pressures just come from different sources. For example, the city of Miami Beach is bound to Florida Department of Law Enforcement (FDLE) accreditation, which is the barometer by which police in the city may apply for federal funding. And then there's PCI. With Joe Citizen paying his taxes, driver's license fees and parking tickets with credit cards, the municipality, like most others, is bound to the industry's payment card security standard.

Nelson Martinez, systems support manager for the city, tackles the intersection of these demands by centralizing the city's IT infrastructure and applying ITIL as a service management platform and NIST standards to address security. This centralization becomes more important in the coming months as the city implements its egovernment initiative, which essentially creates a virtual city hall online.

"Being public funded, there's an ethical issue there. We hold ourselves to a degree of responsibility. We like to be in line with certain industry-wide security policies," Martinez says. "We're pretty much an ITIL shop and we do everything with change controls like private industry. We track everything. We have SLAs."

Martinez's organization is responsible for the city's infrastructure—networks, servers, desktops, gateways, and even disaster recovery. It supports departments with largely mobile workforces such as public safety, which must securely connect, for example, to state and federal databases for background checks during traffic stops.

There are strict FDLE configuration guidelines to which Martinez's systems must adhere, otherwise an incident could not only jeopardize sensitive public information, but endanger the department's ability to procure funding should it fail accreditation.

Standardization under ITIL is crucial,

"We're pretty much an ITIL shop and we do everything with change controls like private industry. We track everything. We have SLAs."

Nelson Martinez, systems support manager, City of Miami Beach

Martinez says. There is one IT department for all city agencies in Miami Beach. "It's truly the only way I want to run an IT shop. Standards are in place. There's a unified security policy that dictates how things are done," Martinez says. "It's the only way we have adequate controls in a heterogeneous environment."

Change controls are the biggest win ITIL affords the security of Martinez's shop.

"You still have to take the initiative to do your scanning and your pen-tests, see where your issues are and fix those," Martinez says. "Once you have established a baseline where you can say, 'I'm for the most part secure,' the change control processes that ITIL says you need to have in place allow you to track changes in your environment."

Martinez says Miami Beach deployed Symantec Enterprise Security Manager to handle its vulnerability scanning and monitor for policy deviations. The tool comes with templates for NIST and NSA standards, for example. Martinez relies on these security templates to map compliance with industry regulations such as PCI and internal policies for mobile connectivity. The city also uses eEye's Blink for real-time IPS and IDS monitoring.

"Symantec ESM is very good at creating our policy templates for servers and tells us whether we're in or out of compliance," Martinez says. "The tool is a good way of showing an auditor that we're doing quarterly audit compliance runs against our machines and remediating."

In the event a security issue threatens the safety of data (and compliance), Martinez says he can resolve it by examining the root cause. Using ITIL, he can determine whether changes in a server or firewall setting, for instance, led to the particular issue.

"It helps you troubleshoot and get back to square one and figure out where this problem was introduced," he says. "If you've got an SLA, how can I guarantee to my customer that I'm going to meet 5 9s for that service?

I need to make sure I am controlling proactively the changes in the environment or making sure those changes are reviewed prior to being implemented."

Martinez says it's vital that risks associated with any change area assessed prior to implementation.

"Change has to be well thought-out," he says. "I believe it's critical to the security and availability of production environments. If you

> "Symantec ESM is very good at creating our policy templates for servers and tells us whether we're in or out of compliance."
>
> Nelson Martinez, systems support manager, City of Miami Beach

do not have adequate change control strategies in place, it's a matter of time before you have a major outage."

Forrester's Othersen says most organizations are in similar straits to these three where they're in the process of adopting frameworks and on their way toward a normalized compliance environment.

"About 10 percent have achieved that nirvana state where they're normalized, their frameworks are rationalized and automated," Othersen says. "The rest are putting down frameworks, getting budgets. There's no procurement or engineering yet, but everyone is getting there. It's just cost inefficient to run things the way they are today."*

Michael S. Mimoso is editor of *Information Security*.

BEST PRACTICES

Consistency Counts

BY RICHARD E. MACKEY

Organizations of all shapes and sizes face compliance requirements from all sides, whether from regulations such as HIPAA, state privacy laws or the Payment Card Industry's Data Security Standard (PCI DSS). • The most efficient and effective way to deal with the diverse set of requirements stemming from the growing array of regulations is to establish a framework of consistent processes and mechanisms. The individual processes can then be adjusted to meet specific regulatory requirements. Here are five best practices that can help organizations fulfill compliance goals across multiple regulations.

Establish an information cataloging and classification process.
At the heart of all regulatory requirements lies information. The information governed by regulations such as HIPAA, PCI and Gramm-Leach-Bliley needs to be protected from leakage and unauthorized access. To successfully protect information, an organization has to know where it is, what makes it sensitive, and who should have access to it. Information cataloging identifies data sets and assigns ownership. Classification defines and documents what makes information sensitive and how it must be handled. These allow an organization to define processes for data handling (e.g., encryption), define process and mechanisms for access control, and establish bounds for what needs to be audited to prove compliance.

Establish a risk management process.
Many regulations require organizations to formally assess and manage risk to protected information and systems. This process needs to be

CONTINUED ON P. 17

CONTINUED FROM P. 16

applied at a high level when businesses change (e.g., in a merger or acquisition) and at a small scale (e.g., when new software or systems are installed). Having a risk assessment and management framework based on a recognized model, like OCTAVE from Carnegie Mellon University, can help organizations meet requirements from multiple regulations and justify strengthening (or weakening) controls.

Develop a consistent identity and access management process.
Every regulation (and auditor) requires organizations to prove they have strong processes controlling who is permitted access to protected information and systems. While this may seem like a largely technical problem, it is primarily a process requirement. Regulations tend to emphasize the requirement that the appropriate people are involved in approving access requests and that there be an audit trail for all requests and approvals. Identity and access management technologies can help with these activities, but they depend on you to develop the appropriate workflows and involve the appropriate players.

Develop a log review process and mechanism.
All regulations require organizations to maintain and monitor logs. Done correctly, logging allows a company to track and prove which users had access to which information, and provides evidence that regular maintenance took place, procedures were followed according to documentation, and certain protections were in place (e.g., firewalls and antivirus). Unfortunately, the challenges facing organizations trying to build and maintain a consistent logging scheme are many. Logs from different products have different formats, are stored in disparate systems, and may include too little or too much information. Organizations need to analyze their logging needs, confront the complexity problem and evaluate event and log management products on the market. The best of these understand log formats from multiple platforms and products, can integrate logs from distributed locations, and can provide powerful analysis tools.

Document your administrative processes.
All regulations require thoroughly documented administrative procedures. However, while many organizations view this requirement to be a compliance burden, it just makes sense. Your organization cannot afford to be placed at risk because the knowledge of how to complete critical administrative functions exists only in the heads of your administrators. There's no shortcut here; the key is to document what you do and then make improvements. There will be a temptation to improve all your processes as you document. That way lies madness. If you want to achieve compliance, document, document, document.

Richard E. Mackey is vice president of SystemExperts.

Key Characteristics of a Federated GRC Strategy

BY MICHAEL RASMUSSEN

A well-executed GRC program reduces the risk of exposure of a firm and creates better business performance.

Governance, risk and compliance (GRC) are interrelated issues affecting organizations. In the past, financial service firms have approached areas of GRC as silos–operational, legal and regulatory risks–operated autonomously of each other.

GRC IS ABOUT ORGANIZATIONAL COLLABORATION

Conversely, firms now strive to develop a more integrated GRC strategy that permeates an organization's processes, decisions and culture. That change demands the sharing of information, assessments, metrics, risks, investigations and losses, all in an effort to reduce business uncertainty and produce predictable results.

This kind of "federated" GRC initiative involves a number of professional roles–the corporate secretary, legal, credit risk, market risk, operational risk, audit, compliance, IT, ethics, corporate social responsibility, and finance. Initial success of a federated GRC program can be measured by the presence of the following characteristics:

- **Sustainability.** Firms demand a sustainable process and infrastructure for GRC requirements that are becoming more sustained and onerous.

"Federated" GRC initiative involves a number of professional roles–the corporate secretary, legal, credit risk, market risk, operational risk, audit, compliance, IT, ethics, corporate social responsibility, and finance.

Further, organizations must assess their risk and compliance management practices on a continuous basis; with the speed of business, point-in-time assessments are no longer good enough and demands that an organization address GRC collaboratively and continuously.

- **Consistency.** Some firms require that multiple roles in the organization work together in an integrated framework. This requires that a common framework be in place so the varying business functions in a firm understand where they fit and how they can share and collaborate data. GRC is getting everyone to play their different positions (roles within the enterprise) from the same playbook. Consistency provides a holistic picture of GRC so that the organization can draw attention to disasters and capture opportunities.

- **Efficiency.** Redundant assessments and audit processes that look for similar information for different purposes are preventing enterprises from getting business done. GRC aims to ease the burden on business areas by leveraging common processes, assessments and information.

- **Transparency.** Financial service firms require transparency across key performance and risk indicators to monitor organizational health, take advantage of opportunity and avert or mitigate disasters. Corporate performance management is tightly related to risk management. When done correctly, performance and risk management are two sides of the same coin.

DEVELOPING A GRC VISION

Once the above-mentioned points are used to determine the basic operational effectiveness of a GRC program, it's time to turn the focus toward long-term strategic planning. The complexity of risk and regulatory demands, as well as the nature of extended and global business, require that some organizations reengineer how they approach silos of governance, risk, and compliance by leveraging processes and information across GRC related business processes.

Developing a successful, long-term federated GRC program involves taking the following steps:

- **Get executive sponsorship.** Firms that try to build their GRC strategy from the bowels of the organization face continual

GRC is getting everyone to play their different positions (roles within the enterprise) from the same playbook.

struggles, typically in the form of internal political issues where GRC becomes a hydra with multiple heads going in different directions. It comes down to a matter of control as these different political heads vie for a leadership position in the GRC strategy. Executive sponsorship alleviates this by establishing a top-down direction. However, the bottom-up strategy still needs to be kept in perspective, as it is the people in the trenches that ultimately need to work in a consistent approach to GRC.

- **Define scope and roles.** GRC is more than enterprise and/or operational risk. A successful GRC strategy is going to start conversations with all the stakeholders in GRC-related domains. Bringing these roles to a collaborative discussion and approach to GRC is what federation is about. A successful GRC strategy starts with defining the charter and vision for GRC and identifying the breadth of business processes and roles that will be incorporated into the GRC strategy.

- **Inventory current systems and processes.** Getting the roles of GRC together leads to the next step of understanding how disparate GRC processes and systems have been implemented. Firms should undertake a detailed inventory of GRC-related processes, systems and technologies to identify where redundancy occurs and establish points of integration.

- **Build your roadmap.** This means identifying short-term and long-term action plans. In the short-term, focus on easy wins to show the value of GRC, as well as pressing GRC issues that the organization is up against (e.g., Basel II, Solvency II, MiFID). For the long-term, develop a plan to integrate the siloed areas of GRC that are not as pressing, such as Sarbanes-Oxley or operational risk.

CONCLUSION

Ignoring a federated view of GRC in today's environment results in business processes, partners, employees, and systems behaving like leaves blowing in the wind. Without a GRC strategy, different parts of the organization end up going in different directions in their respective GRC silos. This leads to wasted resources, inefficiency, a lack of transparency, and significant exposure to the organization. GRC

A successful GRC strategy is going to start conversations with all the stakeholders in GRC-related domains.

aligns them to be more efficient and manageable. Inefficiencies, errors and potential risks can be identified, averted or contained. This reduces the risk exposure of the firm and creates better business performance.*

Michael Rasmussen (mrasmussen@corp-integrity.com) is with Corporate Integrity, LLC. Michael is the authority in understanding governance, risk and compliance (GRC) and is noted for being the first analyst to define and model the GRC market for technology and professional services.

Without a GRC strategy, different parts of the organization end up going in different directions in their respective GRC silos.

Outlining Governance Frameworks

BY ERIC HOLMQUIST

Organizations need to consider many resources and criteria in building a security framework.

The concept of an information security framework is somewhat amorphous, in part because even the phrase "information security" itself can be surprisingly subject to interpretation. At a minimum, a sound framework should provide a blueprint for how information security is governed, define the role of policy and procedure, identify applicable legal or regulatory requirements and support data classification standards and data breach response criteria.

How such frameworks are interpreted and implemented within companies remains wildly varied. For instance, are the controls around sensitive system IDs and passwords part of information security or part of a larger control framework? Is oversight of third parties part of information security or a larger vendor management framework? The lack of clear boundaries creates the challenge.

The answer is both. Information security must be highly integrated into many other operations and control frameworks within institutions.

This tip will briefly describe some of the key principles to consider when building a framework and evaluating a number of standard industry resources against these principles.

MAJOR PRINCIPLES

When evaluating any reference materials for information security governance, the

A sound framework should provide a blueprint for how information security is governed, define the role of policy and procedure, identify applicable legal or regulatory requirements and support data classification standards and data breach response criteria.

following principles should always be kept in mind.

- **Information security must be managed as a business issue, not an IT issue.** Unfortunately, many programs have their roots in IT because IT manages the systems with the most data. However, virtually all compromises are ultimately caused by careless people and poor procedure, not weak systems.

- **It's a team effort.** The governance program must have broad management support, with involvement from senior management, legal, human resources, compliance, audit, risk management and IT.

- **Awareness is key.** The more that people are aware of the risks, rules and their roles, the more they can make the governance program stronger. Information security cannot be managed by a team of experts; it must be everyone's responsibility.

With these principles in mind, we can begin to evaluate the various reference sources that are available to firms to support their own information security governance program.

FFIEC guidelines: The materials given in the interagency guidelines on information security are one of the best resources, and certainly the gold standard for banks. Both the material found in the IT Examination Handbook under Information Security (PDF) and the interagency guidelines are the best available in terms of an overall "program" design and should be the main reference document for every financial institution.

ISO/IEC 27002 (formerly ISO 17799): The international standards document, created in 2000 and subsequently updated in 2005 and 2007, has been an influential tactical document since its creation. The roots of it can be seen in the Information Security section of the FFIEC's IT examination handbook. The cons of the ISO standard are that it is too technology-centric, does not provide a governance framework and includes broader themes of availability and integrity. However, it does contain some of the best data-control categories available and should be a standard-issue reference document for any information security officer.

PCI DSS: Created specifically for the payment card industry, the PCI Data Security

The more that people are aware of the risks, rules and their roles, the more they can make the governance program stronger.

Standard, like the ISO standard, does not provide a governance framework and is heavily IT focused, but it does provide broader language regarding procedural aspects (who has access to data and why). It also includes a detailed checklist that can be useful in designing an internal self-assessment process.

COBIT: While COBIT is a framework document by design, and a very good one, it is not as strong when it comes to information security. It can be an excellent resource for broad IT governance frameworks, but many of the deeper elements of information security management will be found in the above-mentioned documents.

INFORMATION SECURITY GOVERNANCE

Regardless of which materials firms choose as a primary reference, the following concepts are central and critical to building a successful information security governance framework.

Policy: The program should be grounded in a clear, board-level information security policy that positions it as a business issue, mandates the need for a comprehensive program, delegates authority to the role of an information security officer (preferably NOT working in IT) and establishes clear reporting requirements back to the board of directors.

Program: A comprehensive program document that defines: clear roles and responsibilities; discrete program elements; how the overall program is governed; a risk assessment methodology; reporting requirements and testing methodology.

Risk Assessment: A risk assessment methodology that evaluates inherent risks; controls and residual risk to systems; data and physical records; and third parties. It is important to note that each of these four areas will have specific and unique business owners that all must participate in the risk assessment and risk mitigation process.

Policies and Training: The framework should include clear operating polices that outline specific do's and don'ts for managing data, as well as a regular, comprehensive training curriculum that is mandatory for all staff.

Response: A clear and well-tested set of procedures to respond in the event of a data

The framework should include clear operating polices that outline specific do's and don'ts for managing data

breach that, like the program itself, includes both operational and senior management.

The key to information security governance is to remember that the goal is not absolute data restriction. We live with data in motion every day and we cannot do our jobs without the use of confidential data. The goal with information security governance is to build superior resiliency in how data is managed on a day-to-day basis and in our ability to respond should something go wrong.*

Eric Holmquist is the vice president and director of operations risk management at Advanta Bank Corp. He has more than 25 years experience in the financial services industry and is a frequent industry author and speaker. He is responsible for the development and oversight of the bank's operational risk management program.

The key to information security governance is to remember that the goal is not absolute data restriction.

Application Security

PCI Compliance: Addressing Your Needs Via the Database & Grounding at the Database Level

Read about the proven framework for securing data against attack and tampering.

Sarbanes-Oxley (SOX) Compliance from the Database

Discover how DbProtect can bolster SOX compliance efforts by grounding compliance in the database.

HIPAA Compliance and PHI Protection

Learn how DbProtect can strengthen HIPAA compliance and PHI Protection efforts.

Top 5 Database Vulnerabilities Plaguing Federal Agencies

Discover the top five vulnerabilities Federal agencies face and how to correct them.

Security and Compliance: Understand and Address Multiple Requirements

Address PCI, SOX, NIST/FISMA, Basel II and others for greater compliance and reduced risk.

Beyond Trust

Eliminate Admin Rights–Learn more about BeyondTrust Privilege Manager

BeyondTrust enables enterprises to Eliminate Admin Rights and still allow end-users to run all required Windows applications, processes and ActiveX controls.

Locking Down Desktops by Applying the Security Best Practice of Least Privilege

Learn about the security implications of users operating with admin privileges and the different solutions available for least privilege.

How to Build a Secure and Compliant Windows Desktop

Auditors, regulators and business unit owners recognize the threat unsecured desktops pose. Discover how to remove admin rights and increase security and compliance.

Achieve Compliance with IT Audits, SOX, HIPPA, FDCC by Removing Admin Rights

A common goal of many mandates and IT audits is the removal of administrator rights from end-users.

Eliminate Admin Rights–Free Best Practice Webinar Signup

Please join us for an exciting look at how you can eliminate the need to have users run with administrative rights on their workstations.

Lumension Security

Federal Desktop Core Configuration: Achieving Compliance with the Lowest Total Cost of Ownership

Going beyond HIPAA Compliance: Securing the Evolving Endpoint

The Best PCI Audit of Your Life: Are You Ready?

HIPAA and Beyond: How to Effectively Safeguard Electronic Protected Health Information

Endpoint Security Best Practices for Complying with FDCC Standards

MessageLabs

Block Evolving Spam, Secure Your Network

Choosing a Solution for Web-Filtering: Software, Appliance, Managed Service?

Email Security Buyer's Guide: Software, Appliance, Managed Service?

Employee Web Use and Misuse: Companies, Their Employees and the Internet

thawte

Securing your Online Data Transfer with SSL

This white paper provides an introduction to SSL security covering the basics of how it operates and how to deploy appropriate SSL certificates.

Securing your Apache Web Server with a thawte Digital Certificate

Read this white paper and learn more about securing your Apache Web Server with thawte digital certificates.

Extended Validation (EV) SSL Certificates

This white paper details the benefits of extended validation (EV) SSL certificates and how they can help your company.

Securing your Microsoft IIS Web Server with a thawte Digital Certificate

In this guide you will find out how to test, purchase, install and use a thawte Digital Certificate on your Microsoft Internet Information Services (MS IIS) web server.

The thawte Starter PKI Program

Read this white paper and learn about the advantages and benefits of the thawte Starter PKI Program.

Varonis

FISMA, SOX, HIPAA & PCI: Automate. Simplify. Move-on.

Watch this webcast to learn benefits of automating reports on sensitive data to achieve compliance.

10 Things IT Should Be Doing (but isn't)

Read this whitepaper to get the ten must-do actions for maximizing unstructured data protection.

Managing Unstructured Data: 10 Key Requirements

Learn about 10 key requirements to use when evaluating a DP solution for the enterprise.

How Varonis Helps in Sharepoint

Sharepoint is not designed to manage access controls to unstructured data. Varonis can help.

Fixing the "Everyone" Problem: How Restricting Access Can Increase Data Security

Read about the solution that can take care of the "everyone" problem in a matter of mouse clicks.

Websense

Information Security: Meeting Today's Challenges

Controlling Access for File Server Compliance

Managing Email Server Compliance