- ERM - ()

A GRC Blueprint for Strong Risk Management

Developing a standard risk taxonomy, eliminating silos and centralizing risks and controls should be on the checklist of every financial institution looking to establish an effective governance, risk and compliance (GRC) architecture.

Friday, March 11, 2016

By Ryan Rodriguez-Wiggins

Book Review: *null*

Author: Publisher:
Friday, March 11, 2016, By Ryan Rodriguez-Wiggins

Share:

ERM ()

A GRC Blueprint for Strong Risk Management

Developing a standard risk taxonomy, eliminating silos and centralizing risks and controls should be on the checklist of every financial institution looking to establish an effective governance, risk and compliance (GRC) architecture.

Friday, March 11, 2016

By Ryan Rodriguez-Wiggins

Book Review: *null*

Author: Publisher:
Friday, March 11, 2016, By Ryan Rodriguez-Wiggins

Risk management is full of building analogies, and rightfully so. After all, we are trying to build the underlying and sustainable infrastructure that can support global risk management programs — the work of which impacts individuals, businesses, societies and economies around the world.

We oftentimes talk about the “three basic pillars” of audit, risk management and compliance — Rubik’s Cube-like structures that begin at the board or charter level and filter down through risk committees, internal audit and, ultimately, to the business units.

Seldom, however, do we get practical information on what to do next. This is especially pertinent to those banks and financial services organizations that are now facing heightened and unprecedented regulatory scrutiny.

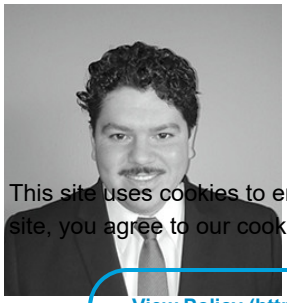
Specifically, smaller sized and community banks come to mind, who may not have the necessary staff needed, required skill sets or technology systems in place to build these robust underlying risk management infrastructures.

Sure, organizations have guidelines and best practices available, but many find themselves stuck on one question: “Where, exactly, do we start?” This question is precisely where a strong governance, risk and compliance (GRC) foundation begins.

Before we get into the how-to of establishing a strong GRC foundation, I would like to begin with the end in mind. Why are we really setting out to do this in the first place?

Textbook Case

In April 2014, Heartbleed (http://heartbleed.com/) was identified as a weakness in the popular OpenSSL cryptographic software library. According to cybersecurity expert Joseph Steinberg (http://www.forbes.com/sites/josephsteinberg/2014/04/10/massive-internet-security-vulnerability-you-are-at-risk-what-you-need-to-do/#78bcfddf58c3), Heartbleed is arguably “the worst vulnerability found ... since commercial traffic began to flow on the Internet.”



Ryan Rodriguez-Wiggins

In the wake of the Heartbleed bug, the IT and risk management teams at one mid-sized bank (a client of ours) had their work cut out for them. They were tasked with the following: (1) identify any and all web-facing assets using OpenSSL; (2) ensure that the latest patch fixing the Heartbleed vulnerability was rolled out across all affected assets; (3) initiate a widespread review of passwords and critical information that may have been exposed; (4) update password security policies; (5) enhance testing policies

and procedures around all open source used within the company; and (6) make certain penetration tests were conducted, ensuring logical outputs for queries and calls.

This bank had already established a strong GRC foundation, so the IT and risk management teams were able to pull together a report for senior management that covered all areas — e.g., product lines, assets, controls and functions — that were susceptible.

While other companies were scrambling to figure out their exposures, this bank was already putting in place specific controls to mitigate risks and the situation was quickly remedied. In the aftermath of Heartbleed, they concluded that a strong underlying GRC foundation was key to their fast, comprehensive response.

The GRC Building Blocks

Small and mid-sized community banks, in particular, share in the common challenge of keeping pace with the evolving volume and velocity of regulatory responsibilities. While most understand the importance of cultivating a risk-aware culture, organizations are not really sure how to build out a program that supports this effort.

Most firms understand the importance of a compliance program that can keep pace with — or even get ahead of — changing regulatory requirements. But they also feel hindered by a lack of budget, experience, technology or even human resources that might be needed.

Risk and compliance aren't exactly rocket science — unless, of course, we look to the quants behind capital modeling programs. Such programs can run the gamut from simple equations to complex Bayesian aggregation and diversification through copulas. But even here, the most basic building block is the unit of measure, without which capital loses its context.

Similarly, we need to understand the basic parts of a company and how it operates: not only the risk and control taxonomies, but also the core components that shape its risk profile.

Centralized List

Typically, the building blocks have been there all along, but are decentralized. It's essential to do a thorough inventory because, without the requisite items, building a GRC foundation will be challenging and prone to stresses.

Start by making a complete, coherent list of your organization's risks and controls. People in different groups may have similar controls but use dissimilar wording, leading to confusion and inefficiency. So make these risks and controls common, using a shared language and taxonomy perspective. We'll explore this in greater detail later.

Second, identify the assets and systems housed within technology groups. These do not necessarily have high visibility to risk management teams, which can be problematic.

Third, align the business units' goals with risk management and ask the following questions: (1) What are all your products and processes? (2) Do you have defined policies and procedures, and, if so, where are all of these stored?

Now that you have collected all this information, put it in a centralized area, so that the risk management group can pull reports from it on a regular basis — or on an *ad hoc* basis, such as when Heartbleed-like incidents occur.

Having this centralized information has further benefits, like empowering the internal audit group to use it for their audit plans. Additionally, when the regulators visit, the compliance group can show there is a common source, housed in one shared (and virtual) location to tie all regulations and responses to inquiries.

A Standard Taxonomy

Developing a standard language and taxonomy that can be found within a "golden source" or a widely-accepted standard will lead to efficiencies later on, such as when the company is doing a risk control self-assessment (RCSA). The more the language and taxonomy conform to what regulators are expecting, the less time you will spend trying to figure out if your program is adequate.

Thanks to Basel, we speak of risk in terms of credit, market, operational and so forth. Within operational risk, for example, there are the seven Basel level 2 risks, such as execution, delivery and process management (EDPM), and business disruption and system failures (BDSF). These are further divided into level 3 risks — such as "model/system misoperation" and "hardware failure" — that may be closer to a company's historical risk categorizations.

Even the experts have qualms about these categories (http://www.opriskadvisory.com/docs/ORA_on_Categorization_-_A_Solution.pdf), but the Basel risks represent the accepted taxonomy. Smaller companies might have a less centralized view of risk, so they might not be classifying risks within those categories.

For example, business disruption might be handled by the business continuity planning group, while system failures might be solely handled by IT. With a well-thought-out GRC foundation, these two functions will be unified in the level 2 BDSF risk. It is important to map your organization's classifications back to industry standards, and this can be done at a level 3 or level 4.

No More Silos

A foundation is built for the whole house; there are not separate silos for the kitchen and bedrooms. In the same way, audit, compliance and risk management should maintain their necessary independence — but not operate in three different silos.

Being able to have all three groups speak the same language allows you to drill down to a specific process, business unit, or product. If one group, for example, says a product is low-risk and the others don't, that disconnect requires investigation.

Great efficiencies can be gained when everyone is speaking the same risk language. Making these common linkages allows for deeper analysis and drives proactive risk management, rather than a simply reactive approach.

Don't Forget About Change Management

After everything is sorted and placed in your organization's GRC library, you want to protect that information, and ensure no changes are made that aren't warranted or agreed upon by the impacted areas. At this stage, we can conclude that the house has been constructed, and we don't want anyone going back into the foundation to make changes.

However, some improvements will be needed from time to time. To add in new risks or controls, stakeholders need to go through a well-defined process. Mapping out ownership, roles and responsibilities internally is key. This segues into a broader change management process.

Change management requires federated ownership and accountability: who owns the change process and who owns the library? Any change will introduce new versions — but how will older versions be denoted and accessed? Resolving these questions is part of change management.

Establish a Global Comparison

One way to put your organization's risk management program in perspective is to compare it against other companies and against the industry as a whole. The Operational Riskdata eXchange Association (https://www.orx.org/Pages/HomePage.aspx) (ORX) is the world's leading operational risk loss data consortium for the financial services industry.

The ORX data follows the Basel taxonomy allowing to at least do some benchmarking. Similarly, other data sources, such as Fitch (https://www.fitchratings.com/web_content/product/FIRST_financial.pdf), provide industry loss data of larger events, using a standard taxonomy for comparison.

In addition to data sources, it is good for program leads to immerse themselves in the broader risk community — via, e.g., attending events and webinars, and participating in general discussions.

Long-Term Sustainability

A house will last only as long as its foundation holds firm. A solid GRC foundation will allow a company to categorize, track and relate risks metrics to one another in a manner that is sustainable and repeatable, quarter over quarter.

When companies are thinking about how to set up their GRC programs, they typically don't know if they want to build technology internally; continue with their existing mode of spreadsheets; or purchase a vendor solution. Spreadsheets are a marvellous invention, and a necessary component to most of our programs; however, they alone do not make for a firm foundation.

At one of my former employers in the banking industry, much of the work was being done in spreadsheets. It was an extremely painstaking process, involving thousands of line items, with different tabs and hyperlinks within a single workbook. With each succeeding quarter, the spreadsheets became more difficult to manage, and thus becoming unsustainable.

Intuitive, predictive, data-driven software can ease the burden: click on one area and a screen pops up with an entire searchable listing. Using such software, you can access information about your GRC foundation anywhere — regardless of your location, platform or device.

Unlike the spreadsheet, there's no chance of deleting a cell by mistake, or mistyping things. It's all categorized and maintained in a safe, secure and sustainable manner. Technology can enable an audit trail (which is important to regulators), whereas using Excel contains certain inherent risks.

Parting Thoughts

Too often, people are driven by the goal of satisfying regulatory concerns. That should be a byproduct, not a driver, of a company's approach to risk management.

A strong risk management program should do more than just answer matters requiring attention (MRAs); rather, it should effect change in the business, ultimately leading to a more profitable and better run and performing company.

Best practices can help unite various GRC functions, such as audit, risk and compliance groups. A federated GRC foundation can break down silos, leverage a standard taxonomy and enable for contextualization and comparison.

Don't wait for the next crisis to hit before taking action now. Start small and start today, and remember that collaboration and continuous improvement are the keys to long-term success. Establish a working group with key stakeholders from the various risk teams and business leads, and empower them to drive the firm's GRC journey.

*Ryan Rodriguez-Wiggins is a senior director of industry GRC solutions at MetricStream. He previously worked as a director of ERM at E*Trade Financial and as a vice president in the operational risk department at Morgan Stanley.*