CHAPTER 4

What first?

Getting started with GRC

Iceberg

So, you've agreed on a vision, you have buy-in from executives and business groups to start moving forward, and you're anxious to get to the first milestone… but what exactly is that milestone?

It's time to start identifying the tactical priorities required to achieve your objectives. For example, one of your objectives may be to *"Establish an enterprise risk management framework"*, but what does that mean to those who are charged with making it real?

Regardless of what corporate objective has been selected to be part of the first work package, there are things that the organization must put in place, and decisions that need to be made, to ensure a successful GRC program. The business groups operating the business, the technology groups supporting the processes, and the management and staff who participate in the program need to be aligned. So let's start with understanding who's on your team, and go from there.

Core competencies

I ask my clients at the beginning of each GRC implementation what they see themselves doing as it relates to the program. Some clients see themselves being users of the solution, and some see themselves being caretakers and developers of their solution. This is a tough question to answer honestly, and if you really think about the implications, it could mean the difference between a successful deployment and one that will fizzle and wither away to a memory. Their answers will help determine where core competencies lie in your organization, and how you can leverage them during various phases of the program.

There are also special skills that may only be required for a short period of time during a long program, so using subject matter experts (SMEs) is often a good way to leverage the precious in-house resources you have at your disposal. These SMEs from outside organizations can actually save money in the long run, since they have been through these large program rollouts before and can arm your team with insights and methods that produce predictable results.

Roles

At the very minimum, the group developing the GRC program should have the role of governance over the program. This will, without doubt, be the single most valuable role the organization can fulfill.

Next would be the counterpart role of Program Manager. In my experience, many organizations limit their success when they underestimate the breadth of these initiatives and treat this program like a project. As I've suggested in a previous

By Kirk Hogan
COO, Iceberg
khogan@icebergnetworks.com

chapter, the difference is that your GRC program will continue to evolve based on its success and positive impact to the organization, where as projects start and end. This changes the mindset dramatically.

Depending on the size and maturity of your organization, there might be solution architects charged with ensuring alignments with standards. There may also be development and testing groups that implement any software or technology.

Another critical role, covered in Chapter 7, is that of the Executive Sponsor. This role provides the mandate and support the groups needs to weather any change of priorities, re-allocation of resources, and expectations.

The foundations of GRC are similar to a building's foundations: you can't build the roof until the basement and walls are constructed.

The importance of Day 2 support

In my experience, the most over-looked role is that of Day 2 support. Has anyone thought of what happens after the program is unveiled to much applause, fanfare and celebration? That first call or e-mail that comes through will require someone to address the inquiry or concern. It may be a knowledge gap, access issue, or confusion about how something works. Having a plan for who to call, for what, is imperative for the ultimate success of a program, and is something that you should be considering up front.

I have seen too many programs with technology components fail because the process was broken, or a role was duplicated and issues arose. It had nothing to do with technology at all. Frustrations mount when Day 2 is not considered, and participants withdraw their support. If they do it openly, then you can address it, but all too often the ones frustrated simply find other ways to meet their objectives without following the program. This certainly spells doom for the overall program, and leadership wears the pain.

Foundations

Foundations must be implemented, or at the very least considered at the onset of any GRC program. Examples of foundations might be process development and maturity. Without these well-described processes, it will be next to impossible to predict the performance of any objective to support the drivers identified. From a risk management point of view, this could be as simple as having an identifiable inventory of controls, and a described process to assess and remediate those controls to satisfy any regulatory or compliance requirement. Common foundational items include:

1. Taxonomy
2. Risk scales, thresholds and frameworks
3. Asset and process inventories
4. Organizational structure
5. Policies, standards and regulations
6. Control libraries
7. Books of Record (sources of truth) within the organization.

You could think of GRC foundations as being very similar to a building's foundation. In the same way you can't build the roof until the basement and walls are constructed, you wouldn't want to inform the Board of Directors that you had a Level 5 risk until you had developed a common language and definition of risk.

Anything that will support a centralized view of the organization model and the things that enable that business to take its products and services to market would be candidates for a foundation. The later processes that will process, analyze and report context are dependent on foundation items being place.

Many organizations want to accomplish the assessment and reporting step without addressing foundations first. But that's not possible if you are also looking for traceability, because without that foundational context, you cannot answer the basic question, *"How do you know?"*

You can't accomplish the assessment and reporting step without addressing foundation first.

Direct and indirect components

Direct components are those items that have a direct relationship with the focus of the GRC program priorities. An example might be an organization that wants to focus on developing their 3rd Party Risk Management capability, where they would identify direct components as their official roster of 3rd parties and any associated engagements. It could also include an inventory of services provided to the organization, and any associated contracts or agreements in place. These might be considered to have a first generation relationship with the priorities.

Indirect components would include anything else beyond the first generation items that could still be considered supporting the program objective, but could also be considered optional. In the example above, an indirect component for a 3rd Party Risk Management capability might be a list of prior organizations where current 3rd Party key executives have worked.

The interesting thing is that organization by organization, the same components could be considered direct or indirect, based on their priorities and objectives. This concept really just helps identify direct components as those that should be dealt with first.

More in this series

Chapter 5 is **"Measuring Value"**. We'll look at how to determine what – and how – to measure the value of your GRC program, so that you can evaluate its value to your organization. More chapters from **Getting Started With GRC** series are available at **icebergnetworks.com/risk-intelligence/**