CHAPTER 1

Where to start?

Getting started with GRC

Iceberg

If you find yourself in a position of responsibility for managing risk at any organization, whether large or small, the journey to achieve insight into your risk posture will be very similar. I would like nothing better than to tell you that the journey is swift and free of challenges, but as you might expect, the truth is much different. The good news is that a pragmatic and high value strategic program is definitely achievable.

I've worked with many organizations that have tried to develop GRC programs, but have approached it thinking that the very smart people who owned risk to begin with were the only resources they needed to conceive and deliver a program that was operational and returned the promised value. In actuality, success requires people with skills and experience gained through practical implementations to ensure success. As you'll read in the coming chapters, success also requires big picture thinking to align your GRC program to the company's strategic goals, along with a focus on building trust and achieving buy-in from various stakeholders.

The GRC value promise

Regardless of what approach, product, schedule, taxonomy, or methodology you plan to use to support your vision for a GRC program, the value promise is essentially the same: Management requires time-sensitive understanding of the pulse of their organization as it relates to the categorized risks and the related controls meant to keep them within tolerances; they need to make informed risk-based business decisions supported by highly standardized technical data; and they need the ability to efficiently respond to regulators and standards bodies with credible and trustworthy demonstration of due diligence and compliance.

The challenge

How can such a small statement describing the value be so difficult to deliver? For one, GRC as a concept is relatively new for most organizations, and the GRC marketplace is still evolving. For example, many products do a very good job at providing useful information for their slice of an ever expanding landscape of technology safeguards employed by organizations to provide the technical controls necessary to manage IT risk. But IT Risk is only one component of Operational Risk, and Operational Risk is only one part of an overall Enterprise Risk program.

The expectation is that management can get a holistic, aggregated view of all types of risk. In most organizations today, risk is assessed and controlled by silos of responsibility, and overlapping or undefined areas of accountability. The challenge therefore becomes merging the outcomes of many different technical controls, process controls, and management controls (policy and governance).

By Kirk Hogan
COO, Iceberg
khogan@icebergnetworks.com

Where to start?

Given that the value promise and challenges are universal, the starting point of a GRC program is as well. Before an organization can make its way forward to a better state of understanding its risk posture at any point in time, it must start with two things:

1. **Understand the current state**
2. **Describe the desired future state**

Before you can move forward, you have to understand your organization's current state and your desired future state.

These are two deceptively simple statements that have the potential to become large and runaway activities. The other factor that must be considered is that while this is the right starting point, most organizations are already somewhere down a path to achieve some better state of managing risk. The activities to determine these two states can be overlaid on any "in progress" program without derailing any current initiatives.

Understanding the current state, or Current Mode of Operations (CMO), allows an organization to take stock of *what* and *how* things are done today. It is conducted through a series of interviews, workshops and internal analysis. By following a structured approach, information can be collected and plotted onto a roadmap as the reference point for evolution.

The desired future state is where organizations get to dream about how things should or could work. Often these take the form of a series of Future Mode of Operations (FMOs) in a sequential form, but they all share the common end state, or vision. We will speak more on vision definition and alignment in another article, so for now it simply serves as *a described state of advanced awareness for management decision making*.

The roadmap

When developing the roadmap, the CMO will be plotted on the timeline indicating the starting position and the FMO plotted at the other end. The effort now is to do the detailed options analysis and prioritization to determine the intermediate milestones to achieve the end state – in other words, the path from "A" to "B". There is a definite order in which these components should be designed and implemented, otherwise you could incur large re-development costs down the road due to re-work to bring the implementation back onto the path.

Next in this series

Chapter 2 is **"The Vision"**, where we'll discuss how to align to common vision, and articulate it so that the people required to support it understand why it's important, and what needs to be done. More chapters from **Getting Started With GRC** series are available at **icebergnetworks.com/risk-intelligence/**