CHAPTER 2

Aligning to a vision

Getting started with GRC

Iceberg

Getting anywhere without knowing where you're going is almost impossible. You can fumble along and eventually make it somewhere (and if you're lucky, maybe even where you decided you wanted to be!), but time and effort will have been wasted in the process. Most organizations have leadership teams with a clear idea about where they want to be, but it's also true that not everyone shares the same priorities in the same way. They also may not be aware of what their peers are doing on a tactical or strategic level.

A vision for your GRC program needs to be clearly articulated so that the people required to support it can understand *why it is important* (how it contributes to or supports the corporate objectives), and *what needs to be done*. Once the 'why' and 'what' have been established, then the 'when', 'where', 'how', and 'who' can be defined.

For many organizations, risk management really boils down to a combination of processes supported by various technologies that implement controls that help handle events. The processes are mostly a blend of manual activities using spreadsheets to collect and manipulate data received from systems and other tools. This approach has a finite lifespan due to the unwieldy nature of managing related data in unrelated spreadsheets, especially in large and dynamic companies.

As organizations with this mode of operation attempt to scale vertically (to handle volume) or horizontally (to handle additional use cases), they soon encounter frustration. There starts to be doubt in the quality and transparency of data that is relied upon routinely to make important business decisions. Once that erosion of trust starts, it's extremely difficult to regain.

By Kirk Hogan
COO, Iceberg
khogan@icebergnetworks.com

Does a vision really work?

Imagine a team of three executives in three separate rooms each being given a million dollars and being told to draw a picture of a house, garage, and driveway that they would build with that money. They're also told that if they can draw the exact same house, garage and driveway, they would only need to build one house, saving two million dollars. It's pretty obvious that unless they coordinate, they will end up creating three different houses, garages and driveways – and spend all of the money.

Now let's change the scenario. Take the same three executives, each with a million dollars, and put them in the same room with a whiteboard where they all create one drawing of the house, garage and driveway. Now they can appreciate eachother's point of view, and work towards compromise, re-prioritization and alignment. In the end only one drawing exists for the house, garage and driveway, and as a result they've only used 33% of the original budget, freeing up valuable resources for other initiatives.

Without exception, all of the enterprise deployments I have been involved in have started with a workshop to align vision and priorities. And each time, even the stalwarts who enter the room with an unmoveable resolve on their priorities, end up at the end of the session with an understanding of why they must move down the list for priorities. The amazing thing is that they offer up this compromise freely because they now appreciate what needs to come first, before their priorities can be successful.

A vision needs to be articulated in a way so that the people required to support it can understand why it is important and what needs to be done.

Soliciting input

Bringing the right people to the table is important for success. Not everyone has to agree — in fact it's good to have different opinions so that people get a view into worlds outside of their familiarity.

I recommend a roundtable workshop format, led by an impartial third party. That way, participants feel that their views are being considered on their own merit without pre-conceived politics or agendas. An impartial facilitator can help keep people out of the rat-holes that consume valuable time. It's also a good rule of thumb not to do too much "solutioning" in this workshop but stay focused on what the business needs as outcomes to support their corporate objectives.

Towards a GRC vision

In developing a vision for a more mature risk management program, most organizations use the following concepts as key parts of their vision:

- **Build confidence** (Executives, Regulators, Auditors)
- **Gain (and maintain) trust** (Customers, Partners)
- **Reduce uncertainty** (Standardized identification of risks to appetite, Metrics driven decision making)
- **Common taxonomy** (One risk language and interpretation of results)

Getting Everyone On-board

You might not get 100% agreement on the objectives or their priority. The important thing is that you expose the roadmap and priorities of different teams so that discussions can happen and executive expectations can be acknowledged. Absolutely everything should be attributed back to the corporate objectives. If something is on a roadmap without being able to describe how it supports a corporate objective, kick it off the roadmap with unceremonious abandon. In short, it needs to make a positive difference.

Next in this series

Chapter 3 is **"How to get there",** about building a workable, prioritized plan, to translate the vision into actionable steps towards the goal. More chapters from this series are available at **icebergnetworks.com/risk-intelligence/**