CHAPTER 8

Essential components

Getting started with GRC

Iceberg

A mature Risk Intelligence program is not about just one thing in isolation. Instead, it is a collection of people, processes and technology, with the right mix based on an organization's level of maturity. It is also about culture and adoption, sponsorship and support. These are the essential components of a GRC program and this chapter will focus on each of them.

Any one of these topics could be expanded upon ad infinitum, so these brief perspectives are really to kickstart your thinking about the state of your program and whether or not these components have the appropriate level of focus and priority.

People

Without people we likely wouldn't need a GRC program! Even with advances in artificial intelligence, people will still be a required component of any risk management program for the foreseeable future. People provide the majority of interpretation of situations, events, information, and results. People are also the reason why so may controls are in place at all. Because the human element is so unpredictable, "what if" planning is largely tied to situations created by humans.

People fall on a spectrum. On one end, some people follow rules with mechanical precision and little deviation, and on the other end you have a predominant creative side where processes are abandoned in favour of free thinking. This spectrum creates the biggest potential for risk, but can also be the source of differentiating approaches to conducting business and taking products and services to market.

The key here is understanding what type of people are in a particular function or role, and adjust either the program or people assignments accordingly.

Process

The component of "process" likely has as many definitions as it does methodologies. I believe that a common definition can be agreed upon, even if the wording is slightly different. If we state that **"A process is a collection of functions, activities and instructions that produces an expected result"**, then it is realistic to expect that the process is streamlined **(efficient)**, and that it yields the expected result **(effective)**, and produces some level of value **(impact)** to the organization.

Being a pragmatist, I work backwards when defining or designing new or updated processes. I believe it's important to first identify what strategic or tactical objective a process will support. By doing this first, we can defend allocating time and money toward it. You don't always have to describe an impact statement with every process, but as an organization matures, it is good practice to do so.

By Kirk Hogan
COO, Iceberg
khogan@icebergnetworks.com

Next will be to design the process to yield a specific result, or set of results regardless of how streamlined it is. The premise here is, "why waste any energy making it efficient if it doesn't work in the first place". Keep tuning the process by adding or removing steps until it produces the result you want.

Process efficiency is specialty all by itself, but in its simplest form, it's about re-organizing and minimizing (or optimizing) steps and effort to the bare minimum while still producing the same result. This can be a bottomless pit of effort if you're not careful, so my recommendation before starting any efficiency work is to define some measurements and capture the current baseline data. From this you can easily demonstrate to those sponsoring the efficiency work that there was a return on their investment of time and money. It sounds simple, but this baseline step is skipped most of the time, and then you have to rely on gut impressions to power through the exercise. Even if the measurement is subjective, measure before and after using the same method.

Technology

Technology is sometimes positioned as the panacea to fix all problems. OK, who are we fooling, that's how it is being positioned almost all of the time these days! We are bombarded all day, every day with new technology that solves a problem we didn't even know we had. The truth is that technology can solve some problems, but you should start first by clearly identifying the problem and understanding what technology and non-technology options you have.

With Risk Intelligence, or any business intelligence, technology can actually help. It may not replace people or processes entirely, but technology can address the volume and velocity challenge most businesses face today. Technology allows us to collect and offer more and more information to help manage the business, moving faster today and even faster tomorrow.

In the realm of managing risk, many organizations start with spreadsheets to handle a relatively small scale of information. This works well until the organization requires scale, either through an integrated program or simply due to the sheer size of the business. Remember that today the typical business extends far beyond its corporate walls (either physical or virtual) into the cloud and through business relationships with partners, suppliers, and clients. This expanded environment needs to be managed with the same rigor and diligence.

In a regulated industry, the regulators also want demonstrable proof of this due diligence, and it typically happens that they ask for proof when you can least afford the cycles to respond to their requests! At this point an organization should be considering a GRC platform to coordinate a more centralized approach to risk management and gather intelligence through an integrated and aggregated lens.

Today the typical business extends far beyond its corporate walls into the cloud and through business relationships with partners, suppliers, and clients. This expanded environment needs to be managed with the same rigor and diligence.

Culture

Having the right people, processes and technology will only support the program, but the program itself is powered by culture. The culture may be one of accountability, or perhaps excellence or awareness. I believe that culture is perhaps the most important component. Without it, you might as well not develop processes or implement technology, because the risks will not be effectively managed, and it becomes a game of *when* things will collapse, not *if*.

Having the right people, processes and technology will only support the program. The program itself is powered by culture.

In my experience working with organizations ranging from local small businesses to Fortune 500 companies, a culture of adapting, learning and transparent accountability has worked best. This honest and open cultural approach identifies issues the quickest and admits they need resolution. It assigns ownership to resolve the problems, and accountability to meet timelines. With a culture like this, an organization can move in an agile fashion and out-compete based on sound risk-based decisions.

I would go so far as to say that hiring people with a cultural fit first, before evaluating skills or capability, may be the best way to ensure that a Risk Intelligence (or any other program) will operate at an optimum level. It doesn't mean you won't screen candidates first by skills and experience, but if they don't fit your culture, move on.

Adoption, sponsorship and support

These next three components are closely tied. **Adoption** is the willingness of the organization to embrace change. This goes against the natural human tendency to avoid or reject change. For an organization to remain competitive and relevant, change is inevitable. This isn't to say that all change has to maintain the same rate or pace, but to not change at all will most likely result in becoming obsolete or working long instead of smart.

Adoption success can be tied to many different factors, but in my experience, **sponsorship,** or leadership, is the single most important factor. If your sponsor or leader does not think change is required, then any effort expended in designing and implementing new processes or technology is wasted. Sponsors must not only believe it is important, but they must make it part of everyday operations, of everyday conversations, and must rely on the new change make decisions. Only then will change become important to all that are expected to effect it.

Building on a previous chapter about executive sponsorship, my only other addition here would be to suggest that a sponsor should clearly identify what strategic or tactical goal this change is tied to. This clear declaration will remind everyone why it was important, and why it remains important.

As important as it is to identify the goal the change is tied to, it is equally important that the organization knows who the champion is. Sometimes the "who" will have enough weight to make the change happen.

Finally, many GRC programs think of all the steps up to the point where it has been designed, built, and turned up. Strangely enough, many forget to plan who will **support** the program on Day 2, once it's live in production.

Support could come in the form of technology support. In this case you may have designed and deployed a GRC platform to support your Risk Intelligence program. Having a team with the right skills and responsiveness will have a huge payback in the initial days of rolling out a solution. Users will have had their day-to-day processes enabled by technology in ways they may not understand, and until they become familiar, the support team is the front line for success.

Support could come from business analysts who understand how things used to work, compared to how things work now. They will have the insight into the reasoning behind why they have changed, and be able to explain the advantages of the change. They will also likely be able to offer alternative routes in the process as long as they achieve the expected result.

Having a team with the right skills and responsiveness will have a huge payback in the initial days of rolling out a solution.

Another suggestion for support is to keep knowledge current. The guide or instructions that applied at the onset of your program are likely to have changed. Nothing confuses users more than getting stale advice or out-of-date information when things have obviously changed. Invest in knowledge transfer during each revision, and maintain a re-usable knowledgebase for new personnel.

RACI awareness

The RACI (Responsible, Accountable, Consulted, Informed) method is a matrix that lists critical activities that must be assigned or monitored, sorting them by role and key function. As with any method, there are variations of RACI, but they attempt to do the same thing: identify expectations.

As you define a program, and as it evolves, it is highly recommended that a RACI be maintained to identify who is who, and who does what. If it's used as a map of who to contact to address issues with, and not as a way to find who is at fault, a RACI can be an effective tool to quickly identify how to keep your program on track, and how to support it once it is running.

Summary

These components are essential regardless of the type of program you are implementing. The same basic truths remain, and considering their relative weight and importance at the outset of the program journey will at least allow you to identify the minimum level for each component.

More in this series

Expectations are high for implementing a risk management platform and what it means for the organization. With those expectations comes the pressure to demonstrate value quickly, and this leads to some common mistakes. In Chapter 9 we discuss the top three mistakes we see on a regular basis, and offer some strategies to help avoid them. More chapters from this series are available at **icebergnetworks.com/risk-intelligence/**