

Getting started with GRC

Helping organizations plan
for a successful GRC program

icebergnetworks.com



Table of contents

INTRODUCTION	3
CHAPTER 1 Where to start?	4
CHAPTER 2 Aligning to a vision	7
CHAPTER 3 How to get there	10
CHAPTER 4 What first?	15
CHAPTER 5 Measuring value	20
CHAPTER 6 Quick wins	24
CHAPTER 7 Executive sponsorship	28
CHAPTER 8 Essential components	32
CHAPTER 9 Top 3 GRC mistakes	38

Introduction

When you deploy a GRC solution, you have a chance to evolve your processes, and mature your organization's culture and approach to risk management. Each chapter in this eBook explores a concept that we've seen to be critical to the success of any GRC deployment, whether you already have a GRC tool in place or you're starting from scratch. This series is written by **Kirk Hogan**, Iceberg's senior GRC consultant and Chief Operating Officer.



About the author

Kirk is responsible for overseeing the delivery, services, strategy and implementation for Iceberg's core offerings. He has developed Iceberg's Centre of Excellence methodologies and *Risk Intelligence Academy* **which is** used to elevate the value of Iceberg services and partner organizations alike. Kirk is an in-house expert providing risk management consulting with our valued customers, where he plays an active role in developing IT security architecture. **Kirk is the** lead facilitator **for** our visioning and alignment workshops — helping some of the largest financial institutions in North America. With more than 25 years of demonstrated experience in the information technology and security industry, Kirk is regarded as an industry expert and frequently speaks at leading security and risk events across North America.

How to use this eBook: Click on the chapters in the tabs at the top to jump to a specific chapter or use the bottom left arrows to navigate through the pages.



CHAPTER 1

Where to start?

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).


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

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



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.



CHAPTER 2

Aligning to a vision

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

spread-sheets 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.

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.

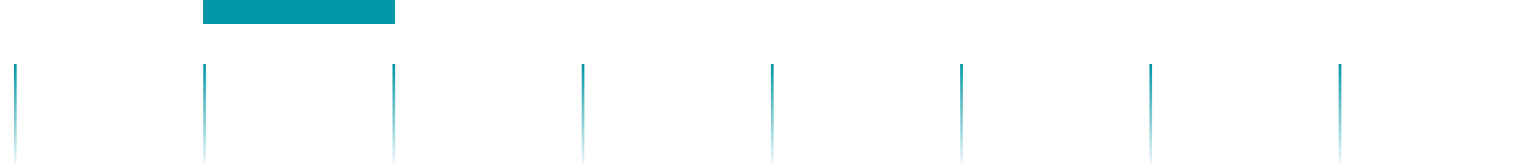
Now let's change the scenario. Take the same three executives, each with a million dollars, and put them in the same room with a whiteboard where they all create one drawing of the house, garage and driveway. Now they can appreciate each other's point of view, and work towards compromise, reprioritization 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.

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.

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.

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.



CHAPTER 3

How to get there

OK, so your organization has held the appropriate workshops to articulate the vision, and now everyone is wondering, “*How do we get there?*”. I’ve worked with many organizations that had the most detailed vision that fully identified characteristics of the end state along with the overall objectives of the program, but they struggled to turn that vision (*strategic*) into action (*tactical activities*). It wasn’t because they didn’t have the talent or skills, but because rolling out a GRC program is something that is outside of their experience and comfort zone.


I would also argue that the overall vision should be broken down to sub-strategies (depending on the size of the program) that support the grand vision. These sub-strategies are what I refer to as “streams”, with each stream being a logical grouping of program components in the areas of:

Use Cases

People

**Policy and/or
Governance**

Technology



Keeping the number of streams to a low number (ideally under six) helps maintain alignment throughout each phase of development and implementation, and therefore inherently reduces the program delivery risk.

The complete roadmap view


If you have ever used a GPS while driving from point A to point B, you can appreciate that looking at only the next turn directly ahead of you may get you there, but you don't get a sense of overall progress, or your relative position to other things around you. By zooming out to get the rest of the map in view, you quickly appreciate where you really are in your trip. The same thing is true for using an overall roadmap for deploying a risk management program. Zoom out a bit and you'll better understand the scale, complexity, duration, participation and budget.

By its very nature, a GRC program is an aggregator of other systems and data. It would not have nearly as much value if it was a stand-alone solution performing all the functions, mainly due to the fact that many of the functions it needs to gather data are already systems operating through your organization. A GRC program is an integrated toolset that brings information, processes, and resources together to provide an aggregated

The real magic happens when all the participants of the GRC program can see and appreciate their role in actualizing the project.

view of all these things, and ultimately helps management make better decisions. It adds transparency and traceability to instill confidence from management and regulators. That is good for business.

There are many roles, across many operational groups, that will appreciate a complete roadmap view. The Program Management Office (PMO) will undoubtedly have more confidence, as the roadmap will speak to the integrated view of all tasks needed to successfully deliver a program on time and budget. The Chief Financial Officer (CFO) will have a better understanding of the resource requirements over time by stream and phase. This view will help them defer costs until they are absolutely needed, but more importantly get a view of Total Cost of Ownership (TCO).



The real magic happens when all the participants of the GRC program can see and appreciate their role in actualizing the project. An aggregated view using the four streams I mentioned above will bring technology groups together with operations, and business groups that will ultimately become users of the solution. It also ensures that the proper governance is applied to each aspect of the complete program so that when the solution is put into service, there will be a clear understanding of roles and responsibilities to ensure deployable success.

Attribution


The concept of attribution can be complex if you really dig into it, but I'd rather err on the side of simplicity. I describe attribution as *"the ability to link something to the objective it supports"*. This means that if I cannot describe how any activity on the roadmap is somehow contributing to the realization of an objective, then I can do one of two things: do a better job of describing its connection; or remove the activity.

We will also come back to this concept of attribution in a future chapter when we discuss measuring value, since we should also be able to attribute an increase in value to a specific thing or set of things. For now however, we will simply need to identify which of the streams an activity or component supports.

Prioritizing Activities — “HVA” or “LVA?”

The **High Value Activity (HVA)** or **Lower Value Activity (LVA)** are concepts that the personal development industry has used for years, but I've adopted them with open arms and propose they are also perfectly suited for program management.

The HVA is fairly self-explanatory, but in the spirit of completeness, I would describe an HVA as “any activity that has an obvious and direct attribution to increasing value of the larger objectives”. An example might be performing incremental backups on a critical information system. By comparison, I refer to LVAs as “Lower Value” and not “Low Value” on purpose.



An example of a LVA might be spending a week changing formatting in an administrative manual that might get used twice a year by a single person. I believe that most activities that are placed on a roadmap or program plan have some level of value, but perhaps their attribution is not as clear as the HVAs, or the degree of improvement is in question. Regardless, having this concept available makes the conversations easier to have when trying to make prioritization calls on what activities trump other activities. That's not to say you couldn't define Medium Value Activities (MVAs) and No Value Activities (NVAs), but I don't think it's necessary. MVAs would automatically become HVAs once all existing HVAs were finished, and NVAs would get removed from the plan once it was confirmed they were not attributable to increasing value.


Work packages

We've identified four streams within a GRC roadmap. If you're familiar with rolling out new solutions, you'll also know that every program goes through distinct phases. These phases will vary depending on what methodology is used, but I would suspect that most programs will either use a Waterfall methodology, or a hybrid of a Waterfall and some other type (perhaps Agile or Extreme).

GRC programs become a part of operational evolution and more and more use cases are supported on the same solution base, delivering more value into the organization.

Assuming this is true, it should also then be possible to group components and activities within each stream to provide modular value, starting with foundation items and evolving to those components or activities which rely on foundation items. This will be particularly helpful when you try to deliver quick wins (discussed later in this series in [Chapter 6](#)) to demonstrate incremental value of the program instead of waiting for the end state to be achieved.

Each work package should be accompanied by a Business Requirements Document, Design Specifications, Test Plans/Cases, and other regular project management artefacts. Each work package could be delivered independently, assuming that any work package inter-dependencies have been identified, and a sequence applied.



The power of the work package is that it lets you define the entire program and its components, and then negotiate each one into a specific work package to meet internal pressures for release dates, program features, or other defined milestones.

Treating GRC as a program

If there is any one lesson we have taken away from countless GRC program deployments, is that they are just that — *programs*. Our experience has shown that once a GRC program is treated like a project with a start and an end, the chance of success or prolonged success is greatly diminished.

There is definitely a start to the GRC program, but the key difference is that there really is no end, it just becomes a part of your organization's operational evolution. More and more use cases can be supported on the same solution base, delivering more value into the organization.

Similar to a Business Intelligence Program, a successful GRC program delivers "*Risk Intelligence*," allowing executives to make decisions that are risk-based and attributable to traceable data and information sources.



CHAPTER 4

What first?


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 them-selves 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 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.

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

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 need to weather any change of priorities, re-allocation of resources, and expectations.



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 with-out 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?"*

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.

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

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.



CHAPTER 5

Measuring value

Do you remember the GRC value promise from the first chapter of this series? Let's re-state it: A GRC program should help management achieve a timely understanding of the organization's risk posture; they need to make informed risk-based business decisions supported by trusted and transparent data; and they need the ability to efficiently respond to regulators and standards bodies with a credible demonstration of due diligence and compliance.


So how exactly are you going to measure your program to see if you're delivering on those promises?

The chameleon

Value is such an over-used term because it's one of those words you can use with-out having any specific definition, or you can have it mean whatever you need it to. This can also work in your favour when describing the difference between "what was" and "what is", and between "what is" and "what could be". Unless you are dealing with tangible objects or described absolute values, this becomes a largely subjective exercise.

If we describe risk as "*uncertainty of an outcome*", then anything that could reduce that level of uncertainty should be equitable to positive value.

I've had great results in describing value in terms of success. I have developed success criteria to allow business stakeholders to define a risk management challenge in terms of either not being able to perform a particular risk management activity; or being able to perform it with less-than-desirable results. Now all we have to do to show value is... do it better!



The other thing I'd like to discuss about value is the granularity of the value statement. In most cases, it should be specific enough that a difference can be described, but not with so much detail that the difference becomes onerous to describe. By keeping the value statement at a coarse level, it is still possible to describe the benefit realized by the before and after.

The measurement debate

So if value is a positive benefit between a before and after state, is it always possible to measure the difference? I would argue “yes”. For those that want to dig deeper on the subject, read the book by Douglas Hubbard *“How to Measure Anything”*. In this book, the author describes using “confidence intervals” to help measure anything. Of course I'm over-simplifying, but the idea is that if you have a before and after state which you know are different, you should be able to describe that difference with either a high degree of confidence, or a low degree of confidence. The important thing is, there is at least some degree of confidence achievable.

Understanding the advantages or pitfalls associated with measurement, there are more reasons to measuring value than to not measure!

The debate usually then becomes about whether it is worth measuring if the confidence is low. I would once again argue “yes”. The reason is that by measuring at all, and identifying why confidence is low, you have a problem that is addressable. Now the focus becomes about increasing confidence, and less about the value equation.

To simply state the expected outcome, we expect the following value equation to be true: **Future state > Current state.**



Methods to measure

Now the fun part. Time to measure. For this we need an example that will demonstrate the equation in action. If nothing else, it will fuel the debate. In the best case though, it will help demonstrate the realization of the original business case.

In many of my engagements implementing GRC programs, there is inevitably a requirement to centralize the source of information to support risk-based decisions. Most clients interpret this to mean amalgamate or aggregate the information used to make decisions into one source so that there is no confusion about where the decision support data came from.

In this scenario, the measurement of success would use the current number of decision-support information sources before implementing the GRC, compared to afterwards. For this example, perhaps we have identified four sources of information. Once the GRC program is in place, we'll have improved that to one centralized source of information.

Simply start with those things that you are asked on a highly regular basis, and develop the measurement that makes sense.

Advantages and pitfalls of measurement

It sounds odd to say there are both positives and negatives related to measurement, after all, why would things always be better? Here are some thoughts:

Advantages

- Demonstrate with empirical data why things are better than before
- Prove the original business case made for performing some activity
- Illustrate incremental progression towards end goals
- Develop common understanding and/or language around what is being measured, and how
- Tune measurement models that can be cross-referred to validate outcomes



Pitfalls

- Metrics can be ‘gamed’ if users understand the correlation between inputs and outputs
- Focus can be too intense on numbers, and less about outcomes
- Reported measurements can be trusted when obsolete if not date-time stamped
- Measurements may be used out of context for other purposes than planned

Summary

Understanding the advantages or pitfalls associated with measurement, there are more reasons to measuring value than to not measure! The pitfalls can be mitigated successfully through appropriate controls, so focus on the good that will come from measurement.

Now the question becomes where to start measuring, and how. Make an inventory of those things that you are asked on a highly regular basis, and develop the measurement that makes sense. Then, declare how you will measure. Almost certainly you will receive comments, good with the bad, but your biggest win here will be that a conversation starts to happen, and focus is brought to the most appropriate areas of your business.

We will discuss more around Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), Key Success Indicators (KSIs) in future chapters, so stay tuned.



CHAPTER 6


Quick wins

Hands up if you've been in a meeting within the last few weeks where some-body has declared they need to see quick wins. I attend enough meetings to hear this multiple times weekly, but rarely does the conversation explore exactly what that means. It sounds great to say (after all, who doesn't enjoy winning?) but please... a little more detail... please!

This chapter is really a guide for the next time you hear that magic phrase in a meeting, and how to arm yourself with better questions to clarify what “quick wins” really mean, and how to know when or if you've won. Focusing on the right wins, and achieving them, is an effective way to build buy-in and momentum for your GRC program.

Defining “quick”

The first thing I would ask is: **“What is meant by quick?”** Let's define if we're speaking about hours, days, weeks or months as a time scale. Then I would ask to describe whether this is an entire component, or a partial component to demonstrate progress towards an end goal. This type of approach sets a team up for success because it realizes that the job doesn't need to be complete, but it does have to achieve some minimum mandatory objectives.



I also believe that quick has as much to do with the “perception” of progress as it does with “actual” progress. I have been involved with programs where a frequent touch-point with stakeholders is a perception of progress, and in other cases programs needed tangible artifacts to demonstrate that same level of confidence.

Often the distinction between a “quick win” and a program milestone becomes blurred. Sometimes they can be the same thing, for example, you may have a new process developed and ready for trials defined as both a milestone and a quick win. It has the power to demonstrate that the course of action will generate real results if it continues to receive support.

Cherry picking

Picking something with a higher chance of success usually makes sense, and yet I have seen things selected for quick wins that have the highest chance of failure due to their complexity. There might be good reasons for that selection, but they need to be clearly communicated, along with the risks involved in achieving them.

My recommendation is to make a list of several quick win candidates, and then review the number of variables within your direct and indirect control. It stands to reason that those things within more direct control have a higher likelihood of success, since you control the risk. The more indirect or independent those variables are, the more risk you run with achieving those wins.

Don’t confuse cherry picking with simply identifying the “easy” things ahead and plotting them on a plan as quick wins. Not at all. There is far more power in identifying objectives that will be hard to achieve. Again, it’s important to clearly communicate the work involved and the potential risks. You may even want to break down more complex tasks into a smaller series of “quick wins”. The goal is to consistently deliver on the goals that you’ve set out to accomplish. This will create a tremendous amount of goodwill to help weather the storms.

Expectations collection

The magic of quick wins is all about aligning with expectations. The challenge is getting everyone on board with just one set of expectations. Normally there are multiple stakeholders, with different agendas. You can fight the good fight and try and align them all, or perhaps a better approach might be to collect all the big ticket expectations and see if any are mutually exclusive. If not, then see how feasible it would be to meet them all.

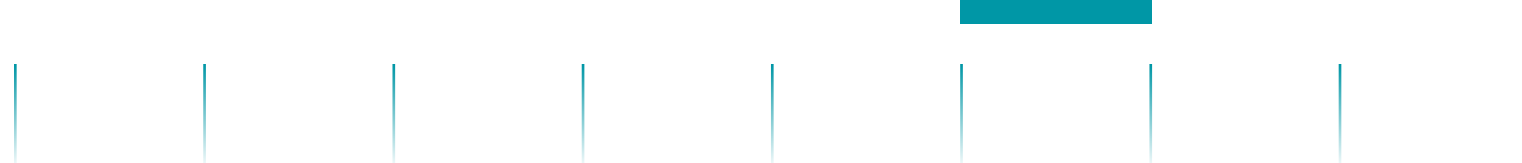
If you can meet all the big expectations, you will have achieved something huge. You will have also likely built a following of fans of your predictable capability to meet objectives, and they will gradually become stronger advocates as the program continues. More than likely though, you will be able to align with a sub-set of expectations. The best scenario would be to have at least one expectation met from each of the stakeholders involved.

Showing a capability to achieve objectives will win you more advocates as the program continues.

The other thing to remember here is that expectations should be managed. While you might be able to demonstrate an end-to-end function, it might not be realistic in early days to operate at full capacity, so temper what will be demonstrated.

Demonstrating value: Preparation is King (or Queen)

In this case, value would refer to “the win”. A typical phrase associated with demonstration of a quick win might look like **“If we could show you that we have re-engineered the process to reduce the effort required and increase its effectiveness, would you agree that continuing to review and re-engineer other core processes would be of value to the organization?”** Making that statement, and knowing that you could demonstrate before and after results through measurements, it would be reasonable to assume continued support — provided the gain justified the expense in resources.



The key however isn't just the quick win itself. Rather, it is the ability to be well-prepared to demonstrate it with great clarity, so that its success is irrefutable. Practice the demonstration, follow a script, develop props or presentations as companions to the demonstration. There is a lot at stake here, so don't hold back! Your demo has to be flawless. Pull that off, and you can celebrate a small victory. Mess it up, and you'll find yourself under a larger microscope.

I have found that identifying several quick wins is even more powerful. In the case where all quick wins are demonstrable within the criteria agreed to at the outset, it is very hard to argue against continued support. The other benefit of multiple quick wins is that you are not at the mercy of just one thing working out. You can create a buffer for success by taking any single event off the critical path, and through a demonstration of a majority of quick wins, that there is value to continue.

Having multiple quick wins along the path of a program will allow you to record each one as they are achieved, and during major milestone reviews, or tough pro-gram status meetings, these lists of wins are like gold. They keep people focused on end goals, and they become less obsessed with the smaller intermediate goals. More importantly, you'll start to see a snowball effect where more and more people (especially the skeptics) come on board and support your broader GRC program vision.



CHAPTER 7


Executive sponsorship

If the success of a risk management or GRC program is reliant on one thing, it's the executive support it needs to flourish. At first that support is required when somebody within the organization articulates the need to be more effective and/or more efficient in managing the ever-increasing levels of threats, vulnerabilities, and therefore risk in the organization. That first person may be taking a career risk suggesting that the organization should evolve, or do things differently than how they're done today. Face it, it's hard to get people to change if the processes they have today are working, even as painful as they may be. The old adage "If it ain't broke, don't fix it" rings loudly.

So how do we effect change in an organization if the natural reaction is reluctance to change? Change can only last if it is a priority from the top down, and that is why executive sponsorship is so central to the success of any program. A GRC program is no different, and in fact I would argue it's actually even more critical to have strong executive support, given the importance of effective risk management in most organizations today.

Sponsorship

The difference between a GRC program with and without a visible and vocal project sponsor is like night and day. Without a sponsor, the short-term priorities of the day take over and the big picture importance becomes less obvious because something else has taken center stage in the conversation. The executive sponsor needs to keep the topic on the table at most meetings, even if only to suggest that other parts of their mandate will be informed by this initiative.



Not to overstate the importance of strong (and visible) executive sponsorship, but it really does make the difference between a program that is effective and successful or not.

Here's the trick though: A sponsor is putting their career on the line to support the program, and the higher the perceived risk, the harder it will likely be to find a sponsor! If your organization is about to make a major pivot like implementing a risk management platform, define the goals that deliver value as quick wins and have a roadmap for additional value in subsequent steps. This approach of incremental risk and reward will help build confidence with the appropriate levels of sponsorship.

The importance of regular updates (no surprises please!)

I reflected on this section for quite a while, and it dawned on me that I know zero executives who have told me, *“I love it when I’m caught off-guard by something and I can’t provide an answer.”* With all seriousness, keeping your sponsor apprised

As much clout as an executive might have, it makes their job so much easier if this initiative is easily attributable to their goals, so that its priority is never brought into question.

of status changes and approaching milestones will build confidence in each phase of your program. Sometimes the updates may be about less-than-desired outcomes, but don't put off updating your sponsor. Inevitably, they will come to hear about the problem at some point, and your quick update cadence will gain their trust that they will get updates regardless of the good or bad news.

You will likely find that by having regularly scheduled updates, they can help unblock obstacles, or provide guidance on how to maneuver challenges. Remember, it is also in their best interest that you succeed.



Attribution to a core mandate

If your priority is not in line with what your executive is expected to deliver or execute, it should come as no surprise that you will get limited support, if any support at all. By ensuring that your conversations, updates and requests are demonstrably aligned with their priorities, you keep the topic on their mind, and more importantly, it becomes part of their daily conversations with other executives. Remember, as much clout as an executive might have, it makes their job so much easier if this initiative is easily attributable to their goals, so that its priority is never brought into doubt.

The core mandates are also the ones with business cases that exist, and with all likelihood have also been supported by an outside consultant who has provided independent verification that the case is sound and justified. This means that the only thing better than being attributed to a core mandate, is being attributed to more than one core mandate. Think of it as an insurance policy.

Do your research, keep your ears open, and find new reasons why your initiative is clearly going to help your executive achieve their objectives if they keep sponsoring your work.

Do your research, keep your ears open, and find new reasons why your initiative is clearly going to help them achieve their objectives if they keep sponsoring your work. Business cases age: what was once critical may eventually become important; what was one important may become elective. Without the business case going through its own lifecycle of updates (which is common), these tidbits of relevance become critical to ongoing sponsorship.



Message development

Do yourself a favour: don't expect that your executive sponsor will have the deep insight you have, or the time to do enough research to develop a compelling message. It is also true that different messages need to be developed for different audiences. Why leave this to chance? Take control and offer some "proposed messaging" and let your executive apply their personal style to your content. Once again, if you make it easy for them to see why they should support you, and you do the heavy lifting developing core content for messaging, they will connect your initiative to probable success.

Check your facts, and check them again. There's nothing that will kill sponsorship like consistently wrong information. Facts and data can also be boring and unconvincing, so develop a story. This is the one thing I have found to be true in all successful initiatives. The story of how this initiative will generate success and further the organizational cause will compel people to listen, be interested, and support. Spend some time discussing what story will fit in with your executive sponsor's other messaging, and ideally you will be able to weave these stories together.

Supporting your sponsor

The reciprocal is also true. As much as you need the sponsorship of the executive, they also need to know that they can turn to you at any time during the program and get the support they need to keep the focus on your program. By this point of implementing your GRC program, your list of "Quick Wins" (see [Chapter 6](#)) should be supplying the executive with ongoing information and validation.

This works in two ways: First, the executive starts to rely on the program itself to get real-time updates, therefore giving them an ever increasing level of confidence that the program is delivering the value that was promised. Second, when the executive makes the GRC program part of their daily operations, it will undoubtedly become an embedded part of many conversations they have with other executive members.

This will have the effect of snowballing support for your program and the value it currently provides, but quite likely you'll find that other executives will start to theorize how your solution might enable their mandate also. What a powerful way to build support and momentum for your GRC initiative.



CHAPTER 8

Essential components

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 many 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.

Next will be to design the process to yield a specific result, or set of results regard-less 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.

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.

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.

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.



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 re-solve 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.

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

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 pro-gram. Having a team with the right skills and responsiveness will have a huge pay-back 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.

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

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.

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 knowledge-base 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.



CHAPTER 9

Top 3 GRC mistakes


Eleanor Roosevelt once quipped: “Learn from the mistakes of others. You can’t live long enough to make them all yourself.” What follows are three mistakes (in no particular order) that I’ve observed throughout more than 20 years of implementing information systems and running large multi-project programs and deployments.

Give these some consideration, taking into account the environment, culture and objectives of your own organization, and you should save yourself countless hours and dollars, and maybe a few grey hairs along the way.

Mistake #1: Working without a vision

A vision is like a map. Without one you have no idea where you’re going, and no way to know if you’re on the right track. With apologies to **Lewis Carroll** (*Alice in Wonderland*), if you don’t know where you’re going, then any road will take you there.

I have had a hand in many projects that didn’t have a well-defined vision in mind, and without exception they have all resulted in less-than-expected results. Without a vision clearly stated, everyone on the project ends up with wildly-varying expectations. You often see competing priorities start to cause frustration and diminished confidence in the project team and their ability to deliver.



Have you ever been on a project with a clear vision? You'll know the difference is astounding, and it's obvious right from the start. The program leader ensures all team members have access to the vision, and likely posts it in clear view for all to reflect on during the project lifecycle. Author **Napoleon Hill** once said, "Whatever the mind can conceive and believe, it can achieve." Re-stated: whatever you can conceive and describe in detail, and then make people believe, can be realized as a vision of what can be.

Some guidelines for creating an effective vision statement:

- The vision statement does not have to be complex or hard to understand, but it should have enough **clarity** to allow those delivering, observing or consuming the goal to know it has been achieved.
- A vision can be a drawing, a detailed explanation, or a goal statement in simple terms: "We will build a 40-foot wall made of brick and mortar, straight as an arrow, and as thick and tall as a man." Granted, the thickness and height of a man can be open to judgment, but it's likely to mean somewhere between 1 and 3 feet thick, and between 4 and 6 feet tall.

A vision should be clear about **what** the GRC solution will do, for **whom** it will do it, and most importantly, **why** you are doing it.

- The purpose of the vision is not to replace specifications, but to **guide specifications** in the right direction. In the example above, if we build a wall 10 feet long, or 6 inches high, we'll know right away we haven't achieved the vision.

Take this GRC vision statement: "Provide visibility into the highest-risk vendors we do business with, and put that information in the hands of the people who manage that risk, so they may implement and maintain appropriate controls." It is clear about what the GRC solution will do, for whom it will do it, and most importantly, why your organization is doing it. This clarity allows everyone involved to test their progress to see how well they are aligned to the goal, and adjust accordingly.

(For more on this topic, see [Chapter 2: Aligning to a vision](#).)



Mistake #2: Underestimating

Have you ever told someone that you'd have a document to them the next day only to find out that the document required more research than originally expected, and constant interruptions stalled your progress for yet another two (or more!) days? We've all been there, and we'll likely do that again in our personal lives.

Estimating for activities during the roll-out of a GRC program requires scrutiny by the program manager during the planning and execution phases. Time and money are in precious supply, and neither can be wasted if the end goal is to be achieved. Not all program sponsors are forgiving enough to approve change requests due to inaccurate or ineffective estimation of activities. I've seen program managers get traded as quickly as the NHL changes coaches after a poor run of games, since they're usually seen as the gatekeeper to accuracy and keeping plans within the bounds of approvals and expectations.

Problems usually arise in areas where you need to depend on other groups for data (information) or participation in workflow and processes. These typically cross political or corporate boundaries and can single-handedly blow estimates. In these cases, doing dry runs of expected flows of information exchange/information sharing should highlight the need for contingency factors that need to be applied.

Technology is an obvious wild card, especially if the organization is trying to connect systems that haven't been connected before. In these cases we usually insist on a prototype phase which literally "proves concepts" before hard estimates are provided. A proof-of-concept does not always have to run end-to-end, but it must remove the unacceptable doubt (or risk) that the estimates will be based on.

In those areas where dry runs or prototypes are not possible, use assumptions to validate estimates. In this way it is reasonable to re-visit estimates should an assumption prove invalid. It should not be used in place of the other methods, but will allow for reasonableness to be applied.

Mistake #3: Skipping the business context

This mistake could be re-stated as “*failure to understand what the business impact could be*”. I have seen some magnificent GRC solutions rolled out to organizations only to watch great disappointment set in once the stakeholders realize they can’t make better decisions based on outputs, or they can’t understand how it ties into their business at all. Much of this can be managed during the design or specification phases, but it must be done in order to demonstrate value to the organization.

The easiest way to ensure that business context is considered is to insist that everything that makes it onto the plan, whether it is an activity or a field on a user interface, has some form of attribution to a **business objective**. By attributing each delivery item to some part of a business function, goal, or expectation, each item can be assigned some level of value. While it’s true that not every individual item needs to be measured, they should in some way support an attributable item.

Ensure that business context is considered by insisting that everything that makes it onto the plan has some form of attribution to a business objective.

With GRC programs, business context can also be stated in the form of **future value**. With a supporting vision and roadmap, items may not provide current value, but could be considered foundation items or building blocks for something of future value. Usually an architecture or design will speak to the sequencing of delivery items and their eventual support of business context.

The business context should not be complicated to understand. With some minor level of explanation, the value to the business should be obvious and attributable.



Learning from the mistakes of others

We really don't get much for free these days, but learning from the mistakes of others falls squarely within this category. I attend industry conferences each year and I find the stories of other practitioners fascinating for so many reasons. Not the least of which are the pitfalls (sometimes very expensive) and lessons learned. In fact, I find that listening to stories from people in industries unlike my own can be just as powerful, because they illustrate how common these mistakes actually are.

My advice is to read a little here and there, meet people at conferences or trade associations, and just ask questions. You'll be amazed how many people would like to share nuggets of knowledge that will spare anyone else their pain!

About Iceberg

We help organizations plan, deploy and support successful Governance, Risk Management & Compliance (GRC) programs. Headquartered in Ottawa, Canada and serving all of North America, our team of consultants, developers and subject matter experts offers a full lifecycle of services, from management workshops to professional services to training and mentoring.

For more information please contact us at
info@icebergnetworks.com or call **855-595-0808**

icebergnetworks.com

