CAPCO

END TO END CONSIDERATIONS FOR GOVERNANCE, RISK AND COMPLIANCE (GRC) TECHNOLOGY SOLUTIONS FOR MID-MARKET BANKS AND CREDIT UNIONS

As banks and credit unions (Organizations) continue to enhance and evolve their risk and compliance frameworks, there comes a time when the conversation moves to "do we need technology to make the process more effective and efficient." This is always a tricky moment because if an organization moves too fast towards implementing GRC technology without having thought-out or completed their internal frameworks, this can result in conflicts, confusion, and a potentially unsuccessful implementation. Governance, Risk and Compliance (GRC) solutions are never the 'silver bullet' to a robust risk and compliance program!

What is Governance Risk and Compliance?

A framework approach for identifying and assessing risks, staying compliant with laws and regulations, and managing strategy. Governance, risk, and compliance frameworks work together to create a forward-looking strategy for an organization.

What is a GRC Technology Solution?

In its simplest form, a technology platform used to capture information, aggregate it using structured organizational hierarchies, processes and common taxonomies to produce output that management can use to make better-informed decisions. It's the enabling of existing governance, risk and compliance frameworks through automation

GRC platforms typically contain a suite of applications that help automate existing frameworks in the bank via disconnected systems or manual forms. The most common applications include risk management, compliance management, IT risk management, IT compliance management, policy management, third-party risk management, audit management, and BCP, to name a few.

This document serves two audiences. Organizations that are considering GRC for the first time and those who have had experiences with a GRC technology solution and looking to enhance an already existing platform or purchase a new one.

Organizations today need to think through their need for GRC technology and what they are trying to accomplish both short- and long-term before investing. In short, codifying what their 'GRC Journey' looks like.

Although every organization's journey looks different, there are some common questions they need to ask themselves to ensure that the path is the right one:

- Are we ready for GRC Technology?
- How do we select the right GRC Platform?
- How do we gain buy-in across the three lines of defense?
- What does an implementation look like, and how do we approach it?
- How do we keep the momentum going post-implementation?

The answers to these questions help frame an organization's next steps!

WHEN IS AN ORGANIZATION READY FOR A GRC SOLUTION?

An institution is typically ready for a GRC solution when its risk and compliance framework matures to a point where technology would promote further efficiency and effectiveness to its processes. A common flaw many institutions make is deciding to purchase technology when their risk and compliance frameworks are non-existent or still being enhanced. Trying to mature a framework while also implementing a technology solution could present major challenges and possibly result in an unsuccessful implementation. Not only does the organization have to implement a risk and compliance program, but now in parallel must learn to use technology.

One initial strategy that organizations should consider is performing a 'framework diagnostic.' For example, a risk management diagnostic would look at program elements such as governance, risk assessment, risk monitoring, reporting, training, and communication, to name a few. The result will be a gap analysis benchmarked against industry best practices and regulatory expectations of where the institution's framework is today and where it needs to be. Any gaps would formulate a roadmap to implement enhancements. A GRC technology implementation would then be a 'phase II' on the project plan. You may be saying to yourself right now, "I don't think we need to do a diagnostic. I think we are ready!" But you may want to take a time out to ensure you really are. If you do, the benefits will be substantial, and the result would be a more usable and sustainable solution that evolves along with the organization's risk and compliance framework.

Another approach would be a 'feasibility study' to identify the basic elements necessary within a risk and compliance program to successfully implement a GRC solution. This is basically a scaled-back version of a complete 'framework diagnostic,' but will help an organization identify the basic elements required to proceed forward and ensure a successful GRC implementation.

An organization also needs to determine its priorities and what you are looking to solve for both the short and long-term. Basically, documenting the 'GRC Journey' of the organization. This roadmap will help you prioritize, set a budget, and ultimately decide what GRC vendors you will want to target for evaluation purposes.

Another critical indicator of readiness for GRC technology is buy-in from the Board and senior management. And not just for budgeting purposes. You want to make them a partner in this pursuit. Keep in mind, they will also reap the rewards from such a system (e.g., better information to make decisions). And in doing so, they may become a user to view reports and dashboards.

To gain management and Board buy-in, make sure they know the value of a GRC solution and how it is distinguished from other technology types such as Board portals and reporting software. Some software is designed for reporting information that is compiled and integrated elsewhere. It is essentially a digital binder of information. It allows users to aggregate data from across the enterprise for more accurate and informed decision making.

WHAT ORGANIZATIONS NEED TO CONSIDER IN SELECTING THE 'RIGHT' GRC SOLUTION?

When you begin your search for a GRC technology solution, a few questions need to be addressed before the evaluation process begins.

They are:

- What problem are you trying to solve?
- What does ultimate success look like? ("you need to know where you are going, to understand and plan how to get there")
- Are you looking for something configurable, customizable, or plug and play?
- Is the solution nimble enough to scale and grow with the organization?

The initial focus should be on the application(s) or module(s) necessary to fulfil the specific need and selecting the GRC platform that satisfies your answers to the above questions. Applications or modules within GRC platforms include risk management, compliance, issues and actions, IT risk, IT compliance, policy management, third-party risk management, BCP, etc.

GRC technology solutions should be considered a long-term strategic play that requires the utmost due diligence during evaluation. This ensures that the right choices are made for the enterprise, taking into-account foundational elements such as relationships between data elements, workflows, and business requirements from all three lines of defense, senior management, and the Board.

When evaluating GRC technology solutions, organizations need to consider the platform's ability to evolve with the organization (i.e., strategic (merger and acquisition), regulatory, environmental factors, etc.) and ultimately be embedded within the fabric of every-day business processes. This is the ultimate GRC success story.

Another factor is whether to purchase a hosted model (SAAS) or an on-premise solution. Cost is a factor. A hosted model is more economical as there will be very little if any technology resources or infrastructure needed from the organization's perspective. It's a straightforward annual license fee from the GRC vendor plus implementation consulting and training fees. An on-premise model is a bit different. The organization may need to pay for additional infrastructure (i.e., internal servers) and devote some technology resource time to support the solution in-house. The on-premise model may sometimes be suitable for larger organizations looking to create a more customized enterprise GRC solution to support their business requirements. Data privacy concerns also come into the mix when deciding between hosted and in-house models. But given the strong information security protocols in place within most GRC vendors, choosing a cloud environment is becoming less of a concern...

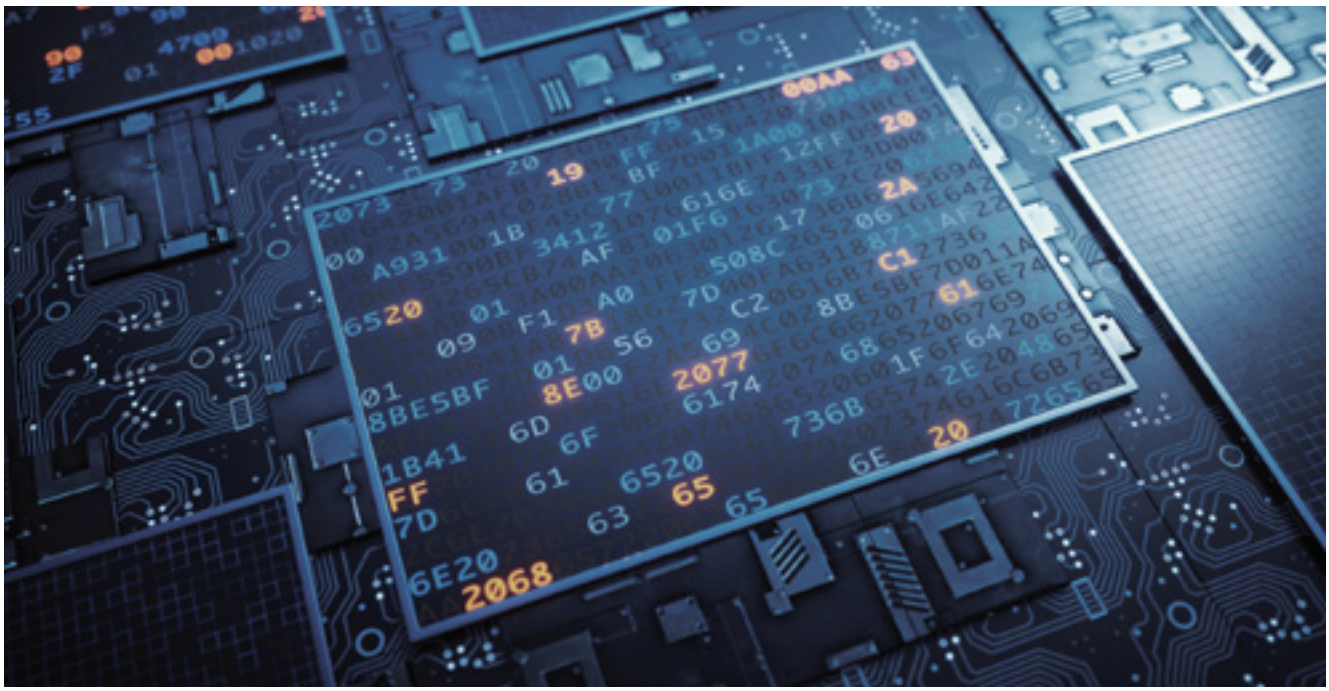
Lastly, supporting a GRC solution post-implementation needs to be a key consideration. In the case of a hosted model, the number of resources will be minimal. Typically, a GRC solution can be supported with one or two parttime internal administrators (depending on the number of applications purchased) to perform administration functions (such as password resets, access rights, as well as maintain/update the hierarchies and GRC content libraries (i.e., risk and controls, policies and procedures, third parties, etc.). In most cases, administrators require assistance from internal subject matter experts and external parties to ensure the application continues to provide maximized value. An alternative option is to outsource support to the GRC vendor or another third party to eliminate the burden on the institution.

In some cases, organizations should think about engaging an independent third party who has the expertise to evaluate the GRC market based on their needs and business requirements. This takes the burden off the organization and provides them with the options to consider in making their important decision.

THE IMPORTANCE OF GAINING THE BUY-IN OF ALL THREE LINES OF DEFENSE

GRC means different things to each line of defense. Most of the time, we see the second line driving the GRC technology purchase, and they sometimes neglect to include the other constituencies into the investment decision. This can have some interesting and undesirable consequences. It isn't uncommon where an organization will have different solutions across the lines of defense. In cases like these, you may not have a path for integration, pay separate license fees, and not leverage a 'one platform' model. The lack of an integrated model over the long term, could lead to redundancies, the lack of common taxonomies across the different solutions and the inability to identify systemic/common themes from the different solutions that management can act on.

A preferred path is an integrated GRC platform where there is a unified foundation, purpose, and goals across all the lines of defense. Although this can be challenging to achieve, it can save money, time, and resources. In cases where the 'one GRC platform model' will not work, thought should be given to integrating some of the common elements so you can maximize value from having multiple GRC technologies. Maybe it is using one of the platforms for enterprise-wide issue and action capture and tracking, or using one solution for managing KRI's, KPI's, KCI's and related metric data.. Strategies like this can get you closer to integration and provide more added value to the organization.



HOW TO APPROACH A GRC IMPLEMENTATION

As with any GRC technology implementation, the key to success is defining the objectives and goals that create a blueprint of "what success looks like" in order to ensure the solution provides functionality and scalability to achieve that end. Then, working backwards, to ensure hierarchies, GRC libraries, objects and configurations are tailored appropriately (based on business requirements), allowing the organization to realize value immediately from the solution.

The right implementation approach is key to establishing a functional GRC technology solution. Below are some key elements for success:

- You should implement a strong, agile project management style. An agile approach to GRC implementations enables rapid prototyping, assists with in-stream UAT, and makes a GRC Solution operational in the client environment.
- Focus on implementing only one to two applications at a time. Phased approaches (focusing on current priorities) ensure small wins that gain buy-in, demonstrate solution value, and pave the way for broader application implementations.
- Having a well-defined business requirements document enables expedited delivery with a focused drive toward the end goal.
- A streamlined project timeline of no more than 20 weeks for one to two applications is reasonable depending upon the number of configurations/customizations involved (e.g., the complexity of hierarchies), GRC libraries (e.g., risk, controls, processes), mapping of the data elements (e.g., workflows, reporting requirements, etc.)
- Establish effective escalation channels to the GRC vendor for risks and issues to keep the engagement moving and on-track.
- Consider leveraging a GRC Implementation Consultant who will do the "heavy lifting". This includes, managing the project (e.g., milestones, budget, status updates), acting as liaison between the organization and GRC vendor, gathering business requirements, establishing foundational elements, mapping data elements, configuring workflows/reports, performing quality control and advising on configurations so output aligns to business requirements ensuring success for the organization.

Successful implementations combine the right balance of implementation expertise and guidance and active participation by all organization stakeholders.

HOW TO KEEP THE MOMENTUM GOING POST-IMPLEMENTATION

Once the GRC solution has been implemented and individuals are trained, the organization needs to start using the solution on a regular basis. The more individuals use and become familiar with the solution, the more they practically understand it and adopt it for everyday use. The organization should create a roll-out plan immediately after implementation or in parallel, outlining clear next steps to begin using the solution. For example, risk assessments, compliance testing, regulatory change management, or whatever the use case may be. Another suggestion is for senior management to announce the 'go-live date,' communicating a reinforcing message outlining the benefits the solutions brings to the organization. This further demonstrates management's commitment and helps to enhance the risk and compliance culture across the organization. In some cases, it can also help tie the GRC solution to a banks overall go-forward business strategy. Organizations that let the solution sit idle after implementation, deal with the need for additional training, along with a delayed roll-out and adoption timeline.

IN SUMMARY

Organizations need to take careful but deliberate steps to determine GRC technology readiness, evaluate, select, and implement a GRC technology solution that fits their business requirements and future state vision. They also need to ensure GRC scalability and sustainability over the long term. If diligent, this process can provide a substantive ROI to the organization in terms of reduced risk and compliance costs, increased operating effectiveness, proactive risk and compliance management and a risk and compliance culture that is tied to business strategy and long-term growth.

AUTHORS

Allan Cuttle, Principal Consultant, allan.cuttle@capco.com
Governance, Risk, and Compliance Practice
Capco RISC Solutions Group
908.907.8127

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO