May 2023

Farm Credit Canada

Best in Class Enterprise GRC Management
Medium Enterprise

CASE***STUDY***

Governance, Risk Management & Compliance Insight

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organisations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

Farm Credit Canada

Best in Class Enterprise GRC Management
Medium Enterprise

The Need for Integrated Governance, Risk Management & Compliance

The physicist Fritjof Capra stated:

"The more we study the major problems of our time, the more we come to realize that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent."

Capra was making the point that ecosystems are complex and interdependent. They require a holistic, contextual awareness of the intricacy of their interconnectedness as an integrated whole, rather than a dissociated collection of systems and parts. Change in one area has cascading effects that impact other areas and the entire ecosystem. The business operates in a world of chaos. In chaos theory, the "butterfly effect" means that something as simple as the flutter of a butterfly's wings in the Netherlands can create tiny changes in the atmosphere that have a cascading effect that can impact the development and path of a hurricane in the Gulf of Mexico. A small event develops into what ends up being a significant issue.

Gone are the years of simplicity in business operations. Exponential growth and change in risks, regulations, globalization, distributed operations, competitive velocity, technology, and business data encumber organizations of all sizes. Keeping business strategy in sync with the accelerated pace of change is is a significant challenge for boards and executives, as well as management professionals throughout all levels of the business.

The interconnectedness of objectives, risks, resiliency, and integrity require 360° contextual awareness of integrated governance, risk management, and compliance (GRC). Organizations need to see the intricate relationships of objectives, risks, obligations, and controls across the enterprise. It requires holistic visibility and intelligence of risk in the context of objectives. The complexity of business – combined with the intricacy and interconnectedness of risk and objectives – necessitates that the organization implement an integrated GRC management strategy.

According to the OCEG definition, GRC[1] is, "a capability to reliably achieve objectives [governance], while addressing uncertainty [risk management], and act with integrity [compliance]." There is a natural flow to the GRC acronym:

1 *GRC official definition in the GRC Capability Model, published by OCEG*

- **Governance – reliably achieves objectives.** The purpose of governance in GRC is to set, direct, and govern the reliable achievement of objectives. Objectives can be overall macro-level but also can be divisional, department, project, process, or even asset-level objectives. Governance involves directing and steering the organization to achieve those objectives reliably.

- **Risk management – address uncertainty.** ISO 31000 defines risk as "the effect of uncertainty on objectives." Good risk management is done in the context of achieving objectives; to optimize risk-taking to ensure that the organization creates value. This is the function of GRC that addresses and mitigates against inevitable uncertainty and threats while operating in a sustainable and calculated manner.

- **Compliance – act with integrity.** The compliance function of GRC is more than regulatory compliance, but the adherence and integrity of the organization to meet its commitments and obligations. These commitments and obligations can be from regulations but also can be found in ethical statements, values, code of conduct, ESG, and contracts.

The Focus is on an Integrated GRC Architecture

The world of business is distributed, dynamic, and disrupted. It is distributed and interconnected across a web of business relationships with stakeholders, clients, and third parties. It is dynamic as the business changes day-by-day and must respond and adapt to evolving environments. Processes change, employees change, relationships change, regulations and risks change, and objectives change. The organization requires a holistic, contextual awareness of GRC – rather than a dissociated collection of processes and departments. Change in one area has cascading effects that impact the entire ecosystem.

This interconnectedness of business drives demand for 360° contextual awareness in the organization's GRC processes to reliably achieve objectives, address uncertainty, and act with integrity. Organizations must see the intricate intersection of objectives, risks, and boundaries across the business. Gone are the years of simplicity in operations. Exponential growth and change in risks, regulations, globalization, distributed operations, competitive velocity, technology, and business data impede the ability of the business to be agile in times of uncertainty.

This challenge is even more significant when GRC management is buried in the depths of departmental processes and addressed inconsistently from different organizational silos and not as an integrated discipline of decision-making that has a symbiotic relationship on the performance and strategy of the organization.

Organizations are focused on developing GRC related strategies and processes supported by an information and technology architecture that can deliver complete 360° insight into risk and compliance. The focus is to deliver:

- **Interconnected risk.** Organizations face an interconnected risk environment and risk cannot be managed in isolation. What started in one area of risk exposure

cascades to others. The recent pandemic has shown, as a health and safety risk had downstream risk impacts on information security, bribery and corruption, fraud, business and operational resiliency, human rights, and other risk areas.

- **Objectives are dynamic.** Adapting to risk events means that businesses need to modify their strategies, departments, processes, and project objectives to address new concerns and possible threats. Objectives become dynamic in reaction to changes in risk exposure. These had to be monitored amid uncertainty in a state of volatility and change.

- **Disruption.** Business is easily disrupted, from international to local events all along the supply chain and extended enterprise. Organizations need to be resilient during disruption with the ability to be agile and resilient in business strategy and operations.

- **Dependency on others.** No organization is an island. The disruption and the interconnectedness of risk impact more than traditional employees and brick-and-mortar businesses but also the range of third-party relationships the organization depends upon, as well as clients. Organizations must address GRC, particularly risk, resiliency, and integrity across the extended enterprise.

- **Dynamic and agile business.** Organizations need to react quickly to stay in business. This requires agility in changing strategy, processes, protecting human resources, employees, and technology. Change also introduces new risks that must be carefully monitored and managed. Organizations need to create an agile foundation that can be flexible in order to meet ever evolving challenges and to bend without breaking.

- **Values defined and tested.** In a dynamic world, organizations strive to align their corporate behavior to ensure their core values demonstrate good corporate citizenship within their communities. From treating employees and customers fairly to how they address human rights such as inclusivity and diversity in their business, operations, and diligence in third-party relationships.

The Bottom Line: In the end, organizations need to reliably achieve objectives, manage uncertainty, and act with integrity and this requires a 360° view of governance, risk management, and compliance within the organization and across its relationships that is supported by an integrated information and technology architecture.

Farm Credit Canada

Best in Class Enterprise GRC Management – Small Enterprise

In the summer of 2018, the manager of Risk Information for Farm Credit Canada (FCC) came back from vacation to find a huge project on her plate. As a major federal lending body for farmers and agricultural enterprises in Canada, FCC had 75 Risk Control Self-Assessments tracked in a 75-worksheet Excel spreadsheet, which were updated quarterly for the board. This sheet was a point of friction for the risk management team, creating

an inefficient and manual process which poorly served the need and was not positioned in a way that added value both locally and downstream.

"Every quarter, we would ask people to attest to the effectiveness of the controls in their shop. We would post that spreadsheet in a SharePoint site so everybody can access it simultaneously." Paulette Beauchesne's team would chase people down via email, ask them to log into SharePoint, and then figure out which of the 75 worksheets was theirs to review. "Scroll down, then there'd be the list of all the controls, and then click a yes or no to the right and if it was a no, then put in an explanation and close the spreadsheet."

The first line of defense hated it. While her team focused on Operational Risk, the Enterprise Risk team would approach many of the same staff a short while later. "For lots of people, there's overlap," explains Beauchesne. Risks that are identified as strategic to the organization are almost always included in a Risk and Control assessment from an operational standpoint. "So Operational Risk would send out this SharePoint site spreadsheet to get an update on the detailed, tactical activities associated with the risk, and then lo and behold, two weeks later, somebody from the Enterprise Risk team would send out an email with a different link asking for an update on the same risk category asking for a higher-level enterprise-wide update on a particular risk. And then, shortly after the end of a quarter, someone from the strategy team is sending out a third email saying, "Provide a very high-level update on the risk that we can include to the risk committee of the board of directors."

Though those three questions looked at risk from different angles, "to the first line of defense, it felt like the same question coming from three people in a one-month span. So that was a big pain point." Between chasing down information, the duplication of work, and not having definitive oversight over problem ownership and accountability (with 75+ risks to self-assess), the process wanted to be thorough but felt cumbersome and inefficient. Reporting took teams a few days to several weeks every quarter. These reports generated few meaningful insights for leadership beyond control failure. When a control inadequacy was identified, there were often significant lags before an action plan was put into place and change occurred.

To address their policy and risk assessment challenges, Farm Credit Canada focused on enterprise GRC management strategy, process, and technology to create a more unified, functional, and agile risk assessment system.

Enterprise GRC Management Strategy

Beauchesne says the strategic shift came five years ago when a new measure was implemented across the organization to close unacceptable risks within a specified time period. FCC leadership noticed a trend that treatment plans to close identified risk gaps were stalling and were not being addressed or closed in a timely manner. "That's what created the risk culture," explains Beauchesne. Having a tangible risk goal presented the need to better track and execute risk control plans from beginning to end and unify these goals across the organization.

Enterprise GRC Management Process

At a round table event, Beauchesne heard someone talking about their GRC journey. "Start where your problem is," said the peer, "Then expand out the other ways. There's no way you can implement everything all at once."

FCC's process problem was figuring out how to meet risk control targets while using a shared spreadsheet and having to "do the math ourselves," says Beauchesne. Beauchesne determined that a process improvement here would make the most significant business impact on the maturity and effectiveness of their risk assessment capabilities. A technology solution would help the teams deliver those improvements with agility and achieve their objectives more reliably while strengthening their ability to develop new solutions in the future.

The FCC team was also willing to review their existing processes while reviewing vendors to see if adaptation was necessary. "We have to be willing to change," says Beauchesne. She encouraged others to keep an open mind while exploring their technology options. "If our procedures are so convoluted that they aren't going to work in this system, let's listen. And maybe it's a time when we could change the order of a process or a procedure."

Enterprise GRC Management Technology

When Beauchesne began looking for an online GRC solution, she put together two guiding principles. The first was to ensure different departments and staff could report once into a central solution and that the information could be used to create multiple types of reporting. "Ask once, report multiple times was one of my guiding principles."

The second guiding principle came from the frustration with the SharePoint process. "The user experience had to be really dead simple," says Beauchesne. Citing the difficulties of getting IT support and time to make changes, Beauchesne knew she wanted the system to be as self-serve as possible and not need many resources to build it out.

They sent out an RFP and picked the top three respondents based on the guiding principles, then asked for a demo looking for three things.

1. How accessible and robust are the tools to do a risk and control self-assessment on a quarterly basis.

2. How clear, relevant, and accessible were the emerging and strategic risk reporting features

3. How would the product integrate with other processes and teams to help centralize and unify risk management efforts?

The FCC team created a rating system for their decision-making committee and scored their options based on the two priorities they had outlined for the decision. They decided to go with the highest scoring solution to their needs, Resolver.

Benefits Delivered

For FCC, Resolver's flexible, no-code solution was a key differentiator. "We wanted no customization, which would typically mean that I'd have to go to my IT department and say, 'Hey, there's a system upgrade tonight. I need resources to make this happen or do an upgrade at our end,'" explains Beauchesne. Knowing the difficulties that can come with needing IT resources, it was critical to the program's success to allow for out-of-the-box solutions that were flexible enough to evolve as programs did. "Resolver's system is highly configurable. Every company does things slightly differently. So when we talked through what our process was, Resolver's Services team could fit the solution to what we need."

This flexibility has empowered Beauchesne's team to be experimental, so when the Resolver team presents a new solution that could improve a program, FCC is willing to see if it works. They've also bought into Resolver's preference for a pilot program. As such, Beauchesne mandates that teams prove a process pilot before building anything in Resolver's platform. "You have to go through a cycle to make sure it works effectively. If it doesn't, you need to review the process because you shouldn't be trying to solve for process problems with software." The team invests their time and effort to ensure a new process is sustainable and works within their new framework instead of relying on bolt-on solutions or workarounds.

Efficiency

The big Excel spreadsheet with the 75 worksheets would take teams six weeks to determine the risk score for each control. According to Beauchesne, implementing the Resolver platform, "We immediately saved six weeks of work at the end of every quarter. Because now we just launched the attestation, which takes 20 minutes on the first day of a quarter, and then people reply within eight days, and then it's live and automatically updated." Report building has become extremely simple. "That's a big win," says Beauchesne.

Beauchesne has redeployed those resources to provide better insights. "We are currently creating different reports that we would have never been able to before having an integrated solution, like Resolver. So instead of spending time doing math on spreadsheets to come up with one number, we can provide more insights." This addressed a key issue with the original process as it only delivered a limited amount of actionable information downstream, especially in relation to the amount of resources it required. With more bandwidth, the team is able to explore new possibilities and create higher value deliverables on a shorter time frame.

"People would ask for something, and we'd just be heads down for three days to get it. And now it's easy."

Effectiveness

By continuing to iterate and add multiple Resolver applications, like internal controls and regulatory compliance, FCC is achieving its goal of reaching the point where "people are reporting into us one time, and then we're using that information for other things." With accessible tools that create concise and unified reporting, the team has been able to both streamline the original process and expand on its results. Delivering higher value information faster and with less effort.

"We've integrated the reporting for Operational and Enterprise risks by asking risk owners to enter comments once into Resolver and populating the information on both the enterprise risk and the operational risk. If the second line of defense needs more color on an enterprise risk at a very high level, they simply reach out to the risk owner to get more information. We have put the extra work on the second line rather than asking the first line to key things in twice." The team has been able to eliminate redundant efforts and reallocate certain aspects to more appropriate owners, this results in a wider scope with a clearer definition, helping the team avoid becoming bogged down in repeat efforts or acting as the involuntary gatekeeper. This clearer definition reduces friction between various stakeholders and helps risk management initiatives maintain momentum throughout their project cycle.

Resolver has helped Beauchesne check off one of her essential guiding principles. "I'd say that the big win is that we are getting to a point where people don't have to report multiple times, or if the internal controls over financial reporting are doing some testing and they notice that a control has failed, they'll automatically inform the Operational Risk team. The RCSA automatically gets updated to say, 'This control is not effective because a control failed testing in the Internal Controls module.'"

Agility

Beauchesne says having a data warehouse in one centralized system has made conversations easier. "Prior to using Resolver, there was this pushback at the end of a quarter to say, 'Well, this control is partly working, so are you sure you can't change this from red to green?' And now those conversations about half-measures and unfinished risk treatment plans are easier." Clarity and unified information allows the team to identify and address problems much faster and with great accuracy. Process mapping and helping to identify key stakeholders is invaluable in ensuring improvement projects and solutions to problems are concluded successfully.

It also meant that FCC could get everybody who needed to be at the table quicker. "When an event or an incident happens, we're able to dive in quickly and figure out who's all touching that process. Whereas we wouldn't have been able to before." When a problem emerges that becomes a crisis, the team can now "go into Resolver and say, 'Here are all the people that need to be in the room because they've identified this process as part of something that happens in their shop." This has replaced the shotgun approach of inviting too many people to address incidents and focuses on precisely who needs to be there, creating more value and efficiency.

The risk culture at FCC and the openness to experimentation mean the team continues to adapt and pivot to problem solve, collaboratively pushing the Resolver team to bring forth flexible solutions to enhance FCC's GRC programs further. "We've done a lot of experimenting. It's like, 'Okay, this is another problem; what can we do to solve it?' For example, we figured out a way to do a strategic risk-ranking exercise in the Resolver platform this past spring. And it's not done through just emails, so I think we're quicker to respond to issues and incidents that come up."

Farm Credit Canada Achieved Best in Class Enterprise GRC Management

GRC is an integrated capability to reliably achieve objectives [GOVERNANCE], address uncertainty [RISK MANAGEMENT], and act with integrity [COMPLIANCE]. Successful GRC strategies deliver the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment. GRC solutions should achieve stronger processes that utilize accurate and reliable information. This enables a better performing, less costly, and more flexible business environment.

GRC 20/20 has evaluated and verified the implementation of Resolver at Farm Credit Canada and confirms that this implementation has achieved a remarkable case study in how to address enterprise GRC management with clear benefits achieved.

This approach is best in class, and in that context GRC 20/20 recognizes Farm Credit Canada and Resolver with a 2023 Best in Class GRC Award in the Category of Enterprise GRC Management – Medium Enterprise (under 1,000 employees).

GRC 20/20's Final Perspective

While FCC's approach to risk is genuinely remarkable, Beauchesne continues to plan for what they are not yet capturing. Things like regulatory compliance that sit outside her team's purview still need to be linked and integrated into Resolver. She's planning business continuity management and third-party risk projects, allowing other teams to dive deeper and proactively plan for risks. FCC will continue to iterate on existing applications and their related processes.

"Some other big areas of what you would call an integrated GRC tool need to be added," Beauchesne describes, ever dreaming up ways to mature FCC's risk practices. "So Incident Management, third-party risk, and business continuity come to mind as things we need to roll into the GRC in some way, shape, or form." With the shift to a centralized, flexible, cloud-based GRC solution, teams will begin to move away from self-assessment for risk, have more robust testing to prove a control works, and move faster to create solutions when they fail.

While there is much work yet to be done to further develop the overall risk management capabilities at FCC, their success after tackling an unsustainable and intolerable process has created a significant amount of momentum amongst the organization. The new

framework for how risk management can be approached, and the evidence to that fact supplied by the results of a single project create a solid foundation from which new capabilities can grow. While the results from the initial project are impressive and well executed, perhaps the most valuable takeaway is the advantageous position for further sustainable development of risk management capabilities FCC has created for itself.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com