☎ 617.624.3600
✉ research@bluehillresearch.com
@BlueHillBoston

BLUE HILL RESEARCH
Translating Technology to Success

Analyst Insight

GRC as an Alternative to Spreadsheets in Enterprise Compliance and Risk Management

Share this Report

What You Need To Know

Governance, risk and compliance (GRC) solutions offer the centralized information management and automated reporting and monitoring capabilities needed to permit organizations to keep pace with the expanding complexity and stakes involved in their enterprise compliance and risk environments. However, despite greater attention to risk and compliance by corporate leadership, organizations face challenges in developing business cases that justify the expense of enterprise GRC implementations. As a result, organizations frequently struggle through disconnected data and manual processes to conduct enterprise risk and compliance analysis, reporting, and audit.

This report draws on research interviews with thirteen organizations to provide a guide for others working through their GRC business case development. This report begins by profiling the costs resulting from spreadsheets and manual processes identified by study participants as well as the corresponding benefits offered by GRC. In addition to providing insight into the business case development process employed by participants, this report profiles six organizations selecting Modulo Risk Manager as their enterprise GRC platform.

Costs and Limitations of Current Practices

To understand the potential impact of enterprise GRC, organizations must begin by assessing the inherent costs and limitations of their present data and process management tools. For most organizations, this means primarily spreadsheet-based, manual processes or disconnected and limited implementations of niche tools supporting a specific function. In particular, as familiar and low cost resources, spreadsheets frequently serve as the default data and process management tools where organizations have not made other investments.

While these tools may be sufficient in low complexity and limited use cases, they often cannot scale to the data, operational needs, and stakeholders involved in enterprise use cases. As such, these tools often force organizations into manual data management and entry, which is time consuming and introduces risks of error and tampering among user chains. As spreadsheet-based processes generally require stakeholders to receive individual versions of files, they also offer limited functionality as uniform repositories of up-to-date data and historical trends. As organizations encounter increasingly complex and changing regulatory and business environments, these limitations begin to generate costs in the form of (1) the productivity of compliance and risk staff, (2) impediments to business execution, and (3) risk exposures. Table 1 summarizes these costs as reported by study participants,

At a Glance

Research Participants:
Thirteen organizations spanning all sizes and industries, including

- Education
- Financial Services
- IT Services
- Manufacturing
- Telecommunications
- Utilities

Common Cost Sources:

- Spreadsheet-based manual processes
- Constraints on risk and compliance productivity
- Impediments to business process execution
- Increased and unknown risk exposures

Impact of GRC:

- Time savings between 25% - 30% in compliance and risk tasks
- Increased visibility into exposures and current performance
- Reduced risk exposure

Table 1: Costs Introduced by Spreadsheet-based and Manual Processes

Costs	Manifestations	Sources
Compliance and Risk Inefficiency	• Time spent entering data • Time spent creating reports • Time spent distributing data to stakeholders • Time spent compiling and reconciling feedback • Time required to respond to inquiries • Time required to respond to auditors and agencies	• Manual data entry and updates • Manual detection and correction of errors • Manual preparation and distribution of documents • Difficulty coordinating multiple stakeholders • Multiple, contradictory or out-of-date versions
Business Operation Interference	• Time spent providing information to compliance and risk • Process delays awaiting approval • Time spent determining requirements • Time spent correcting for requirements	• Multiple, contradictory or out-of-date versions • Manual review and data entry • Manual distribution of documents • Poor retention of information over time • Time required to execute risk and compliance tasks
Risks	• Exposure to regulatory penalties and legal liability • Exposure to regulatory / auditor scrutiny • Exposure to reputational harm • Exposure to poor business outcomes / financial harm	• Mistaken and inaccurate data entry • Opportunity for tampering with data or formulas • Inability to provide information required • Noncompliance with records standards • Inability of compliance and risk staff to take on projects • Poor visibility into up-to-date performance and exposures • Lack of trustworthiness as a record of events

Source: Blue Hill Research, September 2014

Participating organizations most often emphasized how costs resulted from the manual operations involved in spreadsheet use, the difficulty of maintaining a centralized, uniform data repository, and the likelihood of (and difficulty of discovering) accidental entry of incorrect data. The former concerns were most often articulated in terms of their impact on overhead or an inability to keep pace with changing regulations and business operations. This was also said to increase risk exposure, which was the primary concern related to erroneous data entry. Participants also reported great difficulty in locating information requested by auditors and regulators. Organizations with multiple compliance and risk units indicated concerns with contradictory or redundant risk and compliance activities.

> "For us, there's never 'one requirement' we have to meet. We must know and match all requirements that touch each project. We have to worry about ISO 27001. If credit card data is involved, we have to match PCI. For a life sciences client, we worry about HIPAA. To manage all of that in a spreadsheet and a manual exercise -- it takes a lot of time."
>
> - CISO
> International IT Services Provider

Europe-based International Bank: Breezing Through Audit and Reporting with Modulo

The bank's previous network security and compliance solution was only capable of exporting information security data into spreadsheet formats. While satisfied with the underlying solution's performance, the volume and complexity of security data created challenges and excess manual labor in reporting. A report of the bank's 2,000 devices resulted in 60,000 rows in a spreadsheet. The data manipulations and formatting required to translate this data output into usable reports required three days for each report. The bank also found that spreadsheets limited communication between stakeholders, creating additional version control issues adding to delays and potential for inaccurate data. The firm also identified "hidden" infrastructure costs, as large files transferred by email to multiple stakeholders generated a burden for systems and additional lag time for users.

Faced with the resulting inefficiencies and resource drain, the bank implemented Modulo Risk Manager as a middle layer. This provided a centralized "one-stop-shop" facility to slice data, remove unwanted "noise", create and distribute events that could be tracked, and provide performance and assurance reports. The company identified the solution's clearest impact in the reduction of manual effort needed to generate reports, noting that a three-day process now requires approximately one hour of effort. This has freed IT resources to refocus effort on actually remediating events and enabled the process to be extended across the IT infrastructure to improve the risk posture of the organization. In addition, the centralized, streamlined delivery of information has also reduced the time lag for stakeholders as well.

The final area of impact reported relates to audits. In the past, it responded to auditor requests for information with large sets of reports, leaving auditors to search for answers needed. With Modulo, the bank responds with greater precision, which has reduced the time required to complete audits significantly. The bank reports that it now "breezes through" the initial engagement with IT auditors in approximately two hours. It also reports improved transparency and clarity, resulting in greater assurance in interactions with auditors.

Impact of Automation and a GRC Solution

Research participants using GRC to support compliance and risk management uniformly reported that they were motivated by the limitations, data silos, and exposures that resulted from the use of manual processes and spreadsheets. Consistent with the poor information sharing, and retention challenges imposed, these organizations emphasized two aspects of GRC in their investments: (1) process and data management automation, and (2) a centralized, consistent, and controlled repository for compliance and risk information. The value of GRC, in these instances, can be conceptualized in terms of how it helps to reduce the limitations, costs, and risks imposed by prior implementations.

Large North American Utility Provider Uses Modulo Risk Manager to Eliminate Manual Processes

The utility company possesses four separate divisions responsible for managing compliance across the enterprise. Historically, each group employed separate, often spreadsheet-based, processes and standards in support of their areas. This resulted in inconsistent and redundant processes across groups and challenges in gathering and collating data from the various groups for consolidated reporting. All of this required a great deal of manual effort.

Recognizing the obstacles this posed to labor efficiency within compliance groups and to cross-enterprise compliance visibility, the utility sought to develop uniform practices and integrated information management across its compliance groups. It recognized that it would be unable to achieve its objectives without eliminating the limitations spreadsheets placed on consolidating data for consistent reporting across groups and historical insight. The utility selected Modulo Risk Manager to provide a centralized compliance management platform.

> "A spreadsheet is not the slickest tool for reporting. We have a lot of data that had to be downloaded into a CSV. That made for a lot of post-processing in a very unwieldy format before anything could be shared with the team.
>
> Spreadsheets can't match the amount of data we needed and since everything was manually compiled, there's always a worry, not that it was wrong, but certainly that it could be misinterpreted."
>
> - Manager, Security Assurance, Control & Contingency Services; International Bank

The organization has gained improved productivity among its compliance groups as well as improved visibility into enterprise compliance performance. This contributed substantial cost reductions and efficiency gains resulting from the elimination of manual processes across groups. While both the process changes and the replacement of spreadsheets as information management tools with a GRC platform contributed these benefits, the utility attributes 60% of the contribution to GRC.

Study participants using GRC reported these improvements in the form of productivity gains, improved compliance and risk visibility, and reduced risk exposure. To a large degree, these gains originate in the centralized, controlled system of record GRC provides as well as automation in reporting, risk assessment, and other processes (Table 2).

Table 2: Impact of GRC to Replace Spreadsheet-based Processes

	Impact	Resulting from…
Productivity Gains	• Reduction in time spent updating data • Reduction in time spent distributing data • Reduction in time spent compiling data • Reduction in time spent responding to department, regulatory, and auditor requests • Reduction in business process delays	• Uniform and controlled system of record • Automation of processes, alerts, and reporting • Centralized access to compliance and risk information • Ability to customize delivery of compliance and risk data to business context
Visibility & Clarity	• Reduction in errors and inaccurate data • Improved understanding of requirements • Improved insight into changing performance and exposures • Improved insight into decision consequences	• Uniform and controlled system of record • Automation of processes, alerts, and reporting • Centralized access to compliance and risk information • Retention of information and performance data
Risks	• Reduction in exposure to penalties or liability • Reduction in exposure to poor business outcomes and financial harm • Increased trust and "benefit of the doubt" of regulators	• Improved understanding of requirements • Improved insight into changing performance and exposures • Improved ability to demonstrate compliance and efforts made • Increase in risk and compliance projects undertaken

Source: Blue Hill Research, September 2014

Organizations differed in the importance given to these various factors as well as the measures they used to assess the ultimate value of their investments. While profiled organizations relied on qualitative or anecdotal evidence of improvement related to business operations and risk reduction, estimates of time saved in the execution of compliance and risk tasks ranged between 25% and 30%. Organizations reported that this helped to increase the capacity of compliance and risk staff and, in some cases, the reduction in manual work required to complete tasks permitted reductions in overhead.

Overall, estimates of time saved in the execution of compliance and risk tasks resulting from GRC ranged between 25% and 30%.

While often not the primary driver of a GRC investment, this efficiency gain nevertheless played a crucial role in the articulation of the tangible business case for investment (see below) and a measurement of the cost consequences of spreadsheet-based processes. In some cases, these cost consequences took the form of inflated overhead where an abundance of manual activities prompted an expansion in compliance and risk headcount. More often, this consequence manifested as a constraint on the ability of compliance and risk staff to conduct assessments and understand "more strategic" projects that improved the organization's ability to identify, understand, and respond to its exposures.

International IT Services Provider and Consultancy Builds Flexibility and Responsiveness with Modulo Risk Management

Because this organization frequently accesses customer infrastructure, data, and other confidential information in a wide range of industries and across 40 countries, it is extremely sensitive to the data security requirements and industry- and country-specific regulations this entails. The company must maintain standards and security profiles that satisfy the requirements of each of its clients and locations across a broad organization numbering over 140,000 employees.

As a result, the organization manages a large number of differing security profiles with varying levels of security controls to meet each of its clients' requirements for baseline security. Before its adoption of IT GRC, the organization managed these processes manually using spreadsheets. This created extremely time-sensitive work as well as scattered understandings of the organization's risk profile. To this end, the organization observed that performing compliance or risk assessments of even one area of its business was very time consuming and inefficient because it could not understand connections between various data silos or methods of measuring compliance.

As a result, the organization lacked the capability to produce consistent and up-to-date views of its compliance and risk environment. Instead, security consultants and analysts would have to work extensively on a case-by-case basis or for management reporting. This resulted in a great deal of uncertainty for management. It was also a cumbersome process to generate historical views of changing risk and compliance postures of the business units and assets over time.

The organization selected Modulo Risk Manager to provide an enterprise view of risk and compliance. Through the use of the solution, the company has reduced the time required to track down information and generate reports. Beyond that, it cites expanded and timely insight as the solution's greatest impact. Where in the past, the organization was only able to produce reports on a monthly basis; it now possesses "real time" insight into its compliance and risk. Further, it now has a consistent and reliable basis of understanding risk across all business units and assets in the enterprise. In addition to helping the organization to identify issues and areas to focus preventative efforts, Modulo has helped it provide clear and reliable indications of enterprise risk and activities to executive leadership.

"Being a services provider with customers in all industries and coming from all geographies, there is never "one requirement." We have to maintain and manage a number of security profiles to suit the specific needs of our customers. Additionally, we are subject to a number of data protection acts and standards. We needed one unified view of our risk and compliance status against multiple asset classes and standards. We were looking for a solution and a process that can provide risk-based approaches to information. Business units also needed one single dashboard and issue management system to pro-actively manages it security profile. We leverage Modulo Risk Manager to meet this mandate."

- Head of Risk & Compliance
International IT Services Provider

The organization also reported other benefits, including that it:

- Has a diverse information security requirements template (based on its compliance or risk needs) available on a "re-use " model by security analysts and auditors to facilitate consistency in risk management approaches.
- Can create business-relevant quantitative and qualitative reports on identified leading and trailing risk indicators to help prioritize actions and support decision-making.
- Has seen productivity gains when generating risk registers, tracking open issues, and pro-actively managing impending security concerns.

Developing the Business Case

As the prior sections illustrate, while the implementation of GRC entails the additional expense of software investment, its corresponding reduction in the costs *generated* by spreadsheet-based processes means that the spreadsheet is often the more costly solution.

Participating organizations using spreadsheets recognized the limitations imposed by their use but struggled to demonstrate the clear business cases needed to justify investment. By contrast, the organizations that had transitioned to GRC were able to articulate both short-term, tangible gains as well as less easily quantifiable drivers.

The organizations that invested in GRC proved mindful of spreadsheets' limitations and built their business cases. Risk mitigation and improved enterprise insight into risk were primary factors leading these organizations' investment decisions. These factors were reported as offering the greatest value of GRC and the most severe limitation of spreadsheets. However, in each case, these organizations also considered the impact that could be made on compliance, risk, and business operations as more tangible factors related to the investment. In this way, these organizations developed business cases that (1) *justified* the cost of GRC as offsetting the inefficiencies resulting from manual, spreadsheet-based processes and (2) *prioritized* improved business insight and risk mitigation as the ultimate "upside" of investment. This balance permitted these organizations to buttress both aspects of the business case with a more nuanced understanding of the total costs considered as well as a larger vision for enterprise performance.

This multi-faceted awareness also played a role in obtaining the support of various business stakeholders in the investment. While lead by compliance or risk executives, their investment decisions proceeded through committees, bringing together executive leadership as well as audit, risk, and line of business leaders. By emphasizing the specific costs—typically those related to operational performance—related to each one of the affected roles, the organizations were able to build a clear consensus on the investment decision. These organizations also often cited the involvement or support of directors, who were primarily concerned with the business insight and risk mitigation aspects of the investment.

> "Risk management typically gets factored in with perceived critical losses. For example: major loss of services or risk to human life. Even a very savvy, strategically-minded CISO will find it difficult to get a board to buy in to something outside a focus on shareholder fear or media stories. Companies pay attention to what is in the news. That means a lot of effort goes to the loudest needs, not necessarily the most pressing."
>
> - Director Security
> North American Utility

Medical Division of a Large University System Gains Depth of Insight With Modulo Risk Manager

As the medical arm of a major university system, the organization faces an elaborate risk and data security environment with an onerous set of overlapping compliance requirements. The organization's network spans over 170 locations, including administrative offices, clinics, and hospitals stretched over 1,800 miles in a mix of rural and urban environments. The size and complexity of the network, which includes over 16,000 users, created significant obstacles to meaningful cross-organization risk identification and analysis. In particular, the organization reported that it struggled to identify all sources of risk, which caused it to rely on intuition and "best guesses", without ever really knowing its real exposure. As a consequence, the organization reports that it's suffered "a few breaches" over the years, which have generated fines, remediation costs, and some media exposure.

Recognizing that it could not obtain the insight it needed with manual processes, the organization sought out tools to help. It initially used a solution that provided "a good idea where the risk was," but did not provide complete and in-depth comparisons of risk across and between departments. A large part of the challenge resulted from the method used to identify risk. To understand risk within each unit, the organization would need to send surveys to be completed by individual departments and subsequently extrapolate the risk for the department.

Based on these limitations, the organization sought a replacement tool that would supply a deeper enterprise risk view. The organization had also observed other enterprise risk management implementations attempted by the university system that didn't work or were bogged down in deployment delays. As such, the organization prioritized ease of use and implementation time in its selection, looking for a deployment period that "took a couple of months as opposed to a year." The company chose Modulo Risk Manager as tool that could provide the enterprise view needed within a "reasonable amount of time." Competing solutions were found to be "too clunky" or "too complex." While the organization has only had the solution in place for a few months, they report that it has helped to create a deeper insight into risk and is "helping to take us where we want to go."

> "It's a challenge to sell risk to executives. Our corporate mission isn't to solve risk. It's to help sick people. You can strong-arm and be alarmist, but leadership is going to look at you as a joke. If you take a politically sensitive approach to ensure that it's not too burdensome, that it's not getting in the way of the corporate mission, and how you're trying to make it easier for everyone else to do their jobs, that's when you get things done."
>
> - Director of Information Security
> University System Medical Division

Key Observations and Takeaways

The use of spreadsheets to support compliance and risk management results in slow, manual processes, opportunities for inaccuracy and error, impediments to business performance, increased risk exposures, and difficulty in responding to auditors and regulators. It is not difficult to understand how these consequences come about. Rather, the challenge for many organizations lies in determining whether GRC can provide a sufficient improvement to justify the investment expense. The key for organizations is to draw out estimates of the consequences of spreadsheets and compare them with the expenses incurred to invest in GRC solutions.

In building their own cases, organizations will be best served by constructing a multi-faceted assessment of the comparative costs. Organizations that chose to invest in GRC report that operational efficiency gains often helped to justify the cost of the solution, while the most important factors related to the organization's ability to understand and respond to its risk exposures. If the former provided a level of comfort with the cost outlay required to invest in GRC, the latter provided the primary factor motivating the investment.

Authors: Alex Halls, Research Analyst, ahalls@bluehillresearch.com; David Houlihan, Principal Analyst, dhoulihan@bluehillresearch.com

Published: September, 2014