Spreadsheet-Based GRC
The "Universal Tool" Gone Wrong

www.LynxGRC.com

LYNX
TECHNOLOGY PARTNERS

Introduction

In many organizations the genesis of their GRC efforts can be traced back to a few isolated projects that were quick responses to external factors (e.g. scrambling to pass the first PCI audit, "What's this HIPAA thing all about?", etc.) To get these projects going people turned to their reliable "universal tool", the spreadsheet. Suddenly spreadsheets became assessment tools, scoring programs, aggregated databases, report generators, etc. For these projects, spreadsheet-based GRC rose to the occasion and saved the day!

Fast forward a few years. GRC requirements for the organization have increased, and GRC efforts have grown and expanded through almost every department or group. Spreadsheet-based GRC is being called on to handle larger and more extensive GRC efforts. The amount of data being processed is soaring. Assessment and scoring methodologies are becoming more complex. Spreadsheet reconciliation has become a huge-time sink and cost. The universal tool is straining to meet the organization's GRC needs.

Despite these challenges, many organizations using spreadsheet-based GRC feel that staying the course is their best bet. They know spreadsheet-based GRC is not perfect, and they've looked into GRC tools, seen the expected costs, and heard some of the horror stories about transiting to a GRC tool/platform. They've decided change would be too disruptive, too costly, and too risky. But is that really the case?

Have they looked closely at the true complexity of spreadsheet-based GRC and the resulting growth in both costs and risk? As manual GRC processes expand within an organization, the complexity increases dramatically and the cost and risk factors can escalate at an exponential rate. Ironically, cost and risk are two items that GRC theory promises to reduce.

Spreadsheet-Based GRC: Exponential Growth in Both Cost and Risk

Increasing Cost & Risk

Increasing Complexity

COMPLEXITY

As spreadsheet-based GRC is required to handle more advanced and comprehensive GRC efforts, the complexity quickly rises. Because this has happened gradually, over many years, it can be difficult for organizations to see the true level of complexity associated with spreadsheet-based GRC. This complexity impacts processes, scalability, agility, coordination, and communication.

GRC PROCESS AND WORKFLOW

Although data is a critical component, at its core, GRC is a process driven effort. Spreadsheets are data driven. They do not have inherent process and workflow capabilities. Typically, process and workflow is an afterthought in spreadsheet-based GRC efforts. Process documents are posted in various hard-to-find locations, and email becomes the "process and workflow engine." This leads to new employee confusion, difficult process enforcement, and ever-present human error.

SCALABILITY

Given spreadsheet-based GRC's reliance on manual process and the email-based workflow, it can be very difficult to scale to a large organization's complex requirements. Those organizations that try soon find that the percentage of work effort allocated to process tracking and reconciliation dwarfs the actual work of compliance and risk measurement. It is at this point that forward progress on GRC projects begins to grind, sputter, and stall.

AGILITY

Spreadsheet-based GRC starts out very flexible and agile, but as these manual processes spread through an organization, they inevitably become more complex and very rigid. With added process rigidity, organizations find it increasingly difficult to adjust workflows to meet new regulatory requirements. It is also very challenging to increase speed and/or efficiencies in any aspect of their GRC effort. GRC and agility become oxymoronic.

COORDINATION & COMMUNICATION

A critical aspect of GRC processes is that they require the coordination of a large number of people across the organization. Processes and associated progress need to be communicated to large numbers of people to ensure coordination. Spreadsheet-based GRC does nothing to address the complexity of this coordination and communication effort and can even exacerbate the situation.
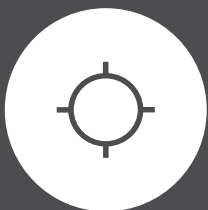
COVERAGE AND SCOPE

Because of the complexity of challenges mentioned above, organizations can be hesitant to expand GRC coverage into new areas. Rather than seeing spreadsheet-based GRC efforts as a net benefit to the organization, they see it as burdensome and strive to limit the scope of GRC to an absolute bare minimum.

COSTS

One of the big initial benefits of spreadsheet-based GRC is the low cost of deployment. Everyone already has spreadsheet software and most workers have basic spreadsheet skills. GRC survey and scoring templates are readily available. Create an internal process document, attach it to a "project kick-off" email addressed to all involved, and the GRC project is off and running - all at minimal cost!

Unfortunately, this simplistic approach to GRC rarely stays this straightforward. In reality, spreadsheet-based GRC in medium to large organizations has very high costs, measured in the form of inefficiencies, data silos, data reconciliation, collaboration limitations, business operations interference, and productivity losses.

INEFFICIENCIES

The manual processes inherent to spreadsheet-based GRC become very inefficient at almost any level of scale. Key areas of inefficiency include, but are not limited to: inaccurate data due to human errors and the resulting need for data checking and redundancy, manual reconciliation of complex spreadsheet models, manual workflow and approval processes, with very limited visibility of progress and state, manual report generation and manipulation, and/or manual distribution of results and correlation of feedback and concerns

BUSINESS OPERATIONS INTERFERENCE

As the inefficiencies due to spreadsheet-based GRC begin to mount, GRC can become a drag on core business operations. Workers spend more and more time away from their main responsibilities, doing GRC-related work. They complain about "GRC spam" and question its value and effectiveness. There is often confusion about what version of the spreadsheet should be used or which process document should be followed. Core business processes are delayed due to required GRC reports and analysis that are not finished. As more and more aspects of spreadsheet-based GRC impact the smooth operation of an organization, the true cost of GRC programs become very visible and increase quickly.

PRODUCTIVITY LOSSES

While inefficiencies of spreadsheet-based GRC has a noticeable impact on employees outside the GRC function, the impact on GRC-centric employees can be catastrophic. These inefficiencies can lead to them spending 50%-80% of their time reconciling thousands of spreadsheets. And to add insult to injury, GRC management typically will find the resulting reports filled with errors from the manual spreadsheet population and reconciliation processes, which spawns yet another data validation and reconciliation cycle.

LIMITED COLLABORATION
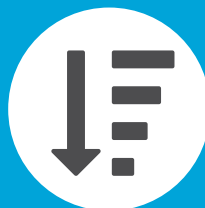
With spreadsheet-based GRC, project participants are challenged in their efforts to work collaboratively. Manual processes, data silos, lack of documentation, etc. all get in the way of collaboration. Because people often don't know who is doing similar work within the project, they lose the opportunity to work together to solve common issues and problems that surface. They also rarely have the opportunity to see "the big picture" and understand where collaboration opportunities may exist.

RISK

As was mentioned earlier, one of the ironies associated with spreadsheet-based GRC is the fact that, in many cases, instead of risk being managed down, it can actually increase. This increase is driven by risk factors such as increased error rates, inaccurate statement of risk/compliance state, lack of an audit trail, and increased auditor scrutiny.
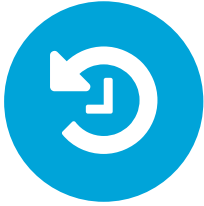
IMPACT OF INCREASED ERROR RATES

Manual processes and total reliance on human data entry and manipulation increase the chance for data errors in spreadsheet-based GRC processes. As a consequence of the compounding affect, the frequency of data errors tends to accelerate with the increasing number and size of GRC projects within an organization. This increased error rate will drive up the probability of errors being associated with multiple critical risk exposure incidents.

INACCURATE RISK/COMPLIANCE STATE

Organizational leaders rely on GRC for accurate risk assessment, scoring, and reporting to effectively manage organizational risk. As the error rate in spreadsheet data increases, the gap between perceived risk and actual risk widens, resulting in an inaccurate executive view of organizational risk and compliance. Efforts to manage organizational risk can become less and less effective, as leaders make decisions based on inaccurate risk or compliance reports.

LACK OF AUDIT TRAIL

With spreadsheet-based GRC it can be difficult to establish and enforce a centralized, uniform data repository where evidence and attestation documentation can be stored. This can create uncertainty and a loss of integrity for forensic analysis of what has been assessed, who assessed it, and the actual assessments and scores. Without a clear, strong audit trail, it is often impossible to ensure that data has not been changed after-the-fact following a risk management incident.

INCREASED AUDITOR SCRUTINY

The risk and compliance impact of spreadsheet errors has not been lost on regulatory bodies, oversight boards, or auditors. Discovery of spreadsheet errors during the audit process can lead to "enhanced audits" that more thoroughly investigate risk and compliance results based on data collected and stored via spreadsheet processes.

Increasing Costs, Risk of GRC Failure

As organizations attempt to scale spreadsheet-based GRC they will encounter increasing levels of complexity that will in turn drive exponential increases in cost and risk. It is highly probable that the increased risk will ultimately lead to a GRC failure, resulting in fines, reputational harm, business disruption, etc. These negative results will counter any perceived cost savings associated with the use of spreadsheets, and will clearly identify the need for a more effective approach to GRC, such as a GRC software platform.

Best Practices for Transitioning from Spreadsheets to a GRC Software Tool or Platform

GRC tool/platform implementation guides and methodologies abound. Every GRC consultant and services provider will tell you their approach is your organization's best choice. To be fair, many of these approaches are based on experience gained from many real-world client engagements, and they could definitely be of value to an organization transitioning away from spreadsheet-based GRC. However, it is important for an organization going through this process to keep in mind a few best-practices specific to the spreadsheet-to-tool transition.

Crawl, Walk, Run

It can be tempting to try get to 100% GRC tool/platform adoption in one pass. Don't do it. There is much to learn and experience in an initial GRC implementation process. Pick a single GRC project within your organization, one that has clear boundaries and can be somewhat isolated. Focus on this project and make it successful. Build on that success by implementing another GRC project. Follow a similar but improved process that has been made better through the experience and knowledge gained in the first implementation. Continue this phased approach until the organization is fully prepared to make a complete transition of all GRC activities onto the appropriate GRC tool/platform.

Configurability

One of the big benefits of using spreadsheets in a GRC process is tool flexibility. Spreadsheets excel (pun intended) in configurability, and because of that, your current GRC process will have become very custom to your organization. It is important that you choose a GRC tool/platform that offers high levels of configurability. Making the transition from spreadsheets to tool/platform will be challenging regardless; do not exacerbate the situation by choosing a tool/platform that cannot be configured to minimize GRC process change.

Guide by the Side

Transitioning from spreadsheet-based GRC to a GRC tool/platform is not easy or straightforward. This is one business change process where having expert assistance pays large dividends. It is important to acknowledge that there will be significant incremental work during this type of transition, and bringing in an experienced and capable GRC services partner will be necessary. However, it is vital to employ a partner that has both the experience to move the project along while effectively transferring knowledge into your organization.

The desired outcome is not to have a "hired gun" come and push the project through to completion. Rather, the goal is to work with your GRC services partner to ensure your organization completes the change over from spreadsheets AND becomes knowledgeable and capable of carrying on independently. This approach allows the organization to have the choice in upcoming phases of GRC tool/platform adoption to selectively deploy internal or external resources as business conditions require.

Conclusion:
It's Time for a Change

If your organization relies primarily on a spreadsheet-based GRC process it is time to make a change. The complex regulatory and risk environment in which businesses must compete has reached a tipping point where GRC processes based on tools like spreadsheets and email cannot meet the challenge. It's time to address your organization's GRC needs with a more modern and purposeful approach and toolset. Do not delay. Start today to build a modern GRC foundation to meet the inevitable, increasing regulatory demands and heightened risk that your organization will most certainly face tomorrow.

IT Risk, Compliance, & Cybersecurity Experts
Fiercely Protecting Our Partners.

Lynx Technology Partners
Address:
1501 Broadway 12th Floor
New York, NY 10036

Website: www.LynxGRC.com
Phone: 1 (800) 314-0455

Email: Sales@LynxTP.com

LYNX
TECHNOLOGY PARTNERS