We need to move on from spreadsheets for compliance and risk management

Simon Marvell
Partner
simon.marvell@acuityrm.com
www.acuityrm.com
+44 (0) 20 7297 2086

Why we use spreadsheets for compliance and risk management

Spreadsheets are a natural first step for organisations that need to measure and report on compliance or assess and manage risk. The drivers for this may be legal, regulatory, internal governance or increasingly from customer demands passing down the supply chain.

Tasked with producing Governance, Risk and Compliance (GRC) management reports, the first instinct is often to turn to spreadsheets which offer the following attractions:

- Licenses are already available for all potential users, avoiding the incremental costs of GRC software licenses
- Very few constraints on content – the user has freedom to design and build a GRC tool that matches the needs of the organisation
- Rapid creation of prototypes – the user can build and develop using an iterative prototyping model and gain agreement at each stage
- Easy distribution and training.

Spreadsheet solutions allow organisations to make a rapid, low-risk start to addressing their compliance and risk management requirements. However, in all but the simplest applications some significant weaknesses in a spreadsheet approach will quickly become apparent

Problems with a spreadsheet approach

- **Scalability** – spreadsheets are fundamentally a single-user tool and while they can be emailed or hosted on a central server they cannot provide the capabilities of a true multi-user tool. If the GRC requirement is to capture and process input from many sources to generate aggregate management reports, this will become a time-consuming and costly process.

- **User Management and Security** – GRC data is often highly sensitive and needs to be segregated so that managers can see their own risk and compliance data but not that of others, resulting in the creation of separate spreadsheets for each business unit. However not all GRC data can be partitioned into business unit 'silos', some is shared - for example non-compliances or weaknesses in a shared systems will have implications for multiple business units. Emailing of GRC spreadsheets and the potential to make multiple copies also raises the risk that sensitive data will be leaked.

- **Errors** – spreadsheets are prone to errors which can be difficult to detect. Although sheets can be locked they may need to be unlocked to provide visibility of data introducing opportunities for error.

- **Change Management** – the use of multiple iterations of spreadsheets to partition data and multiple linkages between sheets results in cumbersome change management when the GRC methodology or content need to be updated.

- **Dependence on the original author** – user developed spreadsheets are often undocumented and dependent on the original author for support and maintenance.

- **Lack of workflow** – Effective GRC requires workflow to manage and coordinate responsibilities for remediation of con-compliances and mitigation of risks - with a spreadsheet GRC solution the workflow activities are usually decoupled from the GRC tool, rather than integrated.

- **Expert systems** – Good GRC solutions will provide a degree of expert guidance and productivity tools to support the user, for example, checklists of risks and controls with relevant mappings to provide assurance that a consistent and repeatable approach is being taken. This is difficult to model in a spreadsheet.

- **Breadth of functionality** – spreadsheets can't deliver the range of functionality of a relational database meaning that there are limitations to the automation of the GRC process which usually have to be compensated for by labour-intensive, and there-fore, expensive manual processes.

Alternative approaches to compliance and risk management

Developing a GRC process can be a challenging and stimulating activity – people naturally like to be given the opportunity to be creative, to produce a methodology and tool at (apparent) low cost that meets the business need and perhaps even advances the 'state of the art'. Spreadsheets are the natural tool to turn to but users should remember that while they are great for exploring ideas and prototyping they are not the solution for long term operational use.

Until recently, the alternatives to spreadsheets have been expensive high-end GRC solutions from the major software vendors, which are only affordable by the largest organisations. To be a logical next step for those wishing to progress from spreadsheets to a commercial off-the-shelf GRC solution the GRC product must offer the following capabilities:

- **Cost** – the entry level cost of ownership the GRC product should be comparable with the cost of ownership of a spreadsheet solution

- **Configurability** – it must be as easy to configure the GRC product with risk, controls, incidents and other GRC data items as it is a spreadsheet

- **Ease of use** – the GRC product should be intuitive to understand, deploy and use with the minimum of training required

- **Valuable, actionable output** – the GRC product should provide added value in its output and reporting which clearly provide incremental benefit over the spreadsheet solution.

Products such as STREAM Integrated Risk Manager from Acuity Risk Management www.acuityrm.com provide an attractive, low-cost alternative to spreadsheets for GRC, scalable from free single-user to Enterprise – wide deployment for the largest organisations.