Calling time on compliance spreadsheet overload

by Richard Hibbert, CEO, SureCloud

Assessing risks of a supply chain is largely performed by old-fashioned methods of spreadsheet questionnaires. This manual, laborious method becomes impossible to manage, even when recruiting an army of skilled compliance officers, who then spend most of their time chasing spreadsheet responses. This can be resolved by a Cloud-based system that provides self-validating forms to the appropriate suppliers' personnel. The system reports on progress and - analyses results, providing vital information on best-performing lower risk suppliers. Such a system makes spreadsheet overload a thing of the past.

Richard Hibbert is cofounder and CEO of SureCloud®, a provider of Software-as-a-Service Governance, Risk and Compliance Solutions. Prior to founding SureCloud, Mr Hibbert held a range of senior executive positions at high technology organisations in the UK, mainland Europe and North America, where he led sales, marketing and market development functions.

Mr Hibbert began his career in IT management consultancy, where he worked for blue chip corporations in the UK, mainland Europe and the USA. In 1995 Richard founded RCL, an IT management consultancy, which specialized in the implementation of ERP applications and the provision of IT managed services. In March 2000, he sold RCL to Morse Computers PLC - a FTSE 350 company - where he continued his employment as Commercial Director of Morse Business Applications.

Today, in addition to leading SureCloud and overseeing the continual innovation of the SureCloud platform, Mr Hibbert advises enterprises on their governance, risk and compliance practices.

Introduction

As the focus on data protection continues to grow and high profile breaches make regular front page news, organisations are examining ways to improve methods for auditing risk among their suppliers and trading partners.

The most common method of assessing supplier risk is through a self-assessment questionnaire (typically delivered by email in a spreadsheet), which is sometimes followed up by an on-site audit. The first step in this process is to determine which set of questions you will use to assess the risk. It makes sense for the organisation to base the questions on those already used to assess internal risk and compliance, whether that is based on ISO27000, the Payment Card Industry Data Security Standard (*PCI DSS*) or any other regulatory standard, not forgetting the opportunity to ask some additional questions specific to the organisation's own working practices and requirements. In reality, there isn't a common supplier self-assessment questionnaire, which means that the majority of organisations use non-standard spreadsheet templates to run this type of audit programme. As we will see, this not only impacts the organisation performing the audits, but also the organisation being audited - resulting in spreadsheet overload.

The great digital paper chase

Organisations operating supplier assurance programmes sometimes underestimate the impact that running such programmes will have on resources. Each programme is generally coordinated by the internal compliance team, whose primary responsibility is to drive the organisation's own compliance objectives. As mentioned in the introduction, it makes sense to take the internal assurance requirements and direct them at the supply chain - after all, the objective is for suppliers to protect data to the same level required in-house, at least. The internal spreadsheet is then 'tweaked' to ask additional questions and the programme is ready for launch.

Consider an organisation with ten suppliers, which means having ten versions of the internal spreadsheet placed with suppliers to be completed. As soon as the Send button is clicked, the organisation has lost visibility and therefore control over the process. Did the spreadsheet get to the intended recipient? Have they opened it? Have they started to answer the questions? What is the quality of the answers? When will the spreadsheet be sent back? These are all questions which cannot be answered without manual follow-up and that means skilled compliance managers essentially engaged in admin - an extremely inefficient use of valuable

resources. As each spreadsheet is returned, the manual process of assessing risk begins. Some questions will not have been answered sufficiently and other questions may not have been answered at all. Manual follow-up, typically by email is again required.

The analysis that can be performed using spreadsheets is limited to each individual spreadsheet. If I want to rank my suppliers by risk, or want to understand common areas of non-compliance or best/worst performers, then I have to undertake an extremely labour-intensive process of summarising spreadsheets to deliver that insight. Now consider an organisation with 1,000 suppliers or more - the challenges can very quickly spiral out of control. Not to mention adding that additional question to each spreadsheet that was overlooked at the programme outset.

The lack of automation adds up to a huge administrative burden. Not only is it inefficient but the sheer number of disparate pieces of data makes analysing the results also difficult. The upshot is that you have very skilled people in an organisation doing a lot of administration, chasing people, making sure that they received their questionnaire, that they understood it and know the deadline for returning it. You end up with a mass of box-ticking but no way of telling who is performing best or which suppliers are leaving the organisation exposed to the most risk.

The evolving regulatory landscape

In the USA, where the Enron and Worldcom financial scandals gave birth to the Sarbanes Oxley Act (often shortened to SOX) in 2002, the consequences for non-compliance with regulatory obligations can spell large fines or imprisonment for the board-level executives responsible. This is in stark contrast to the rest of the world where punishments have tended to focus on fining culpable organisations rather than individuals.

The result has been a lack of executive backing and funding, with companies preferring to use 'home grown' spreadsheets to manage compliance, rather than more robust process-driven solutions. This approach has proliferated across many standards and regulations, to the point that it is no longer scalable. It is a burden on the very professionals that introduced them, who are unable to perform their jobs properly without disproportionately recruiting new heads.

However, a shift in the regulatory landscape is very much on the cards. In the UK, for example, the Information Commissioners Office has started to issue large fines to companies that fail to protect personal data. Furthermore, the UK government does not believe that companies who outsource information to third parties are properly assessing the risk. To combat this, they are promoting the adoption of standards such as ISO 27001, which clearly states the need to protect data held by third parties.

Elsewhere, the EU is becoming increasingly concerned about the rising number of cyber-attacks on government and industry by hostile governments and mafia-style cyber-criminal gangs. A proposed EU directive for Data Protection, whereby companies will have to immediately disclose when they have had a breach, is set to be brought in in 2014. Fines of up to 2% of business turnover could be imposed if the proposed legislation takes effect.

This means that there is now an immediate need for businesses to take ownership for the security of their data and to consider their strategy for doing so. When this happens, the intensity with which the industry polices itself will increase significantly, forcing risk management professionals and budget holders to agree finally that the compliance by spreadsheet approach is no longer acceptable.

Automate the assurance process

One of the most effective ways to improve in-house supplier assurance activity is to lift the whole process into the Cloud. An IT Governance, Risk and Compliance (*GRC*) platform delivered as a Software-as-a-Service allows organisations to automate the auditing process, devolving responsibility for completing questionnaires or sections of questionnaires to those most qualified to provide the answers, for example HR, Finance or IT, and centralises evidence collection. This immediately removes any need for lengthy spreadsheet-based programmes and frees up highly skilled compliance and risk personnel from time-consuming project administration. Cloud-based platforms dramatically reduce the total cost of ownership for IT GRC solutions. They are simple to implement and open up lower points of entry, thereby significantly reducing the risk of project failure.

Furthermore, compliance teams can analyse the entire result-set from the combined supplier responses to deliver intelligence back to the organisation. By analysing the data collected, more informed decisions can be made allowing the audit experts to further de-risk the organisation. For example, some very useful questions can be answered, such as: which are my worst performing suppliers? Do I want to continue to trade with them? Which compliance requirements are all of my suppliers struggling to meet?

Industries such as financial services and retail are starting to benefit from this new found ability to gain unprecedented insight into their supplier assurance programmes.

Automation via the cloud brings a variety of benefits, including:

Ability to implement your own supplier questionnaires or leverage supplied template questionnaires including supplier risk calculations;

Retaining full control over the entire supplier assurance program, by providing access to questionnaires in a central system, with real-time information on progress;

Fine grained permissions to provide different form views based on Stakeholder Groups;

Integrated Task Management to alert users to events such as compliance certificate expiry, or to allocate activity to internal or external stakeholders;

Grouping structures to organise suppliers for example by industry or company size;

Interfaces with common business intelligence tools such as Microsoft Office pivot tables for slicing & dicing data and creation of 'what if' scenarios;

Dashboards and reporting to provide real-time updates on progress;

Analytics to identify patterns, such as top or bottom performing suppliers;

Coordination of supplier assurance with risk management activities.

Conclusion

Senior managers have for too long relied on spreadsheets for all kinds of compliance and risk management processes, from supplier assurance questionnaires to incident responses and management reporting. These processes are inefficient, labour intensive and delivering results that are not fit for purpose. SureCloud advocates a collaborative approach to compliance using a cloud-based model. The approach is agile enough to accommodate any existing processes, allows auditors to see at a glance the status and progress of their programmes and incorporates business analytics for assessing which parts of the supply chain are the most vulnerable. The days of compliance spreadsheet overload are numbered. Senior management urgently needs to grasp this by dropping the inherent inefficiencies and false economies of the old ways and embracing the agile and devolved approach available via the cloud. ●