

# Spreadsheet Risk Management



## Frequently Asked Questions Guide



# Table of contents

<b>Introduction</b>	<b>1</b>
<b>An introduction to spreadsheet risk management</b>	<b>2</b>
1. Why are spreadsheets so prevalent today?	2
2. What is spreadsheet risk management?	2
3. Why do spreadsheets present a risk?	2
4. Is the level of risk increasing?	4
5. What about other desktop tools available to users?	4
6. Why has spreadsheet risk management suddenly become important?	4
7. Do technology solutions exist that can assist with managing spreadsheet risk?	4
<b>Executive ownership and governance</b>	<b>5</b>
8. Who is accountable for effective spreadsheet risk management?	5
9. What do the major legislative acts have to say about spreadsheets?	5
10. How can the executive define and communicate their spreadsheet risk management requirements?	5
11. Who should operate spreadsheet risk management processes?	5
12. Why should we report on spreadsheet risk to senior management and the executive?	6
13. What should the risk responsibilities of a spreadsheet owner cover?	6
14. What should be the role of the IT department?	6
15. What should be the role of operational risk departments?	7
16. What should be the role of internal audit?	7
<b>Creating a library of critical spreadsheets</b>	<b>8</b>
17. How do we measure risk?	8
18. How do we start to identify the potentially critical spreadsheets?	9
19. Which parts of the organisation can have the greatest dependency on critical spreadsheets?	9
20. How can we ensure that we identify all potentially critical spreadsheets?	9
21. What about spreadsheets that have links to other spreadsheets?	10
<b>Implementing a spreadsheet control framework</b>	<b>11</b>
22. What is a spreadsheet control framework and why is it important?	11
23. What are the typical key components of a spreadsheet control framework?	11
24. When is a spreadsheet not fit for purpose?	12
<b>Assessing spreadsheet controls and current risk exposure</b>	<b>13</b>
25. Do we need to assess the controls in operation across all our spreadsheets?	13
26. How do we consistently assess controls across spreadsheets?	13
27. How do we assess whether the controls are effective?	14
28. Can different approaches be taken to resolve any control issues?	14
29. How can we identify common control issues across the organisation?	15
30. How do we ensure that control issues are resolved and closed within an acceptable timeframe?	15
31. Who is responsible for accepting the residual risk that exists within a spreadsheet?	15
<b>Gaining assurance over critical spreadsheets</b>	<b>16</b>
32. How can the organisation ensure that spreadsheet owners are appropriately managing spreadsheet risk?	16
33. Where controls have been deficient, how can we rely on the integrity of the spreadsheet?	16
34. Is it possible to rely on the spreadsheet risk management process to provide assurance over the critical spreadsheets?	16
35. How often should spreadsheets or the spreadsheet control environment be evaluated?	17
36. Should internal audit be relied on to provide assurance on behalf of the business?	17
<b>Spreadsheet risk indicators and reporting</b>	<b>18</b>
37. What other forms of assurance can we rely upon rather than periodic controls assessments?	18
38. Are there generally accepted key indicators of spreadsheet risk or measures that should be applied?	18
39. What information is provided to the executive/risk committees regarding spreadsheet risk?	18
40. How can we ensure management and spreadsheet owners take on more accountability for the risk associated with the spreadsheets they own?	19
41. How can we ensure that spreadsheet risk is incorporated into our current regulatory reporting processes?	19

# Table of contents (continued)

<b>Training and awareness</b>	<b>20</b>
42. Making spreadsheet owners aware of the potential risk is difficult. Are there any tried and tested approaches?	20
43. Are there differing levels of training required for spreadsheet owners?	20
44. Is the intranet an effective tool for ensuring awareness of spreadsheet risk within the organisation?	20
<b>Resources</b>	<b>21</b>
45. What are the key spreadsheet risk management capabilities that should exist in any organisation?	21
46. To what degree should the organisation expect to be sourcing third-party skills?	21
47. Should the organisation be employing specific spreadsheet support teams?	22
48. Should formal processes exist to ensure that the organisation consistently manages spreadsheet risk?	22
<b>Technology enabling effective spreadsheet risk management</b>	<b>23</b>
49. Do technology solutions exist to help with spreadsheet risk management?	23
50. Are there established solutions and clear market leaders?	23
51. If technology solutions are implemented, will they impact all spreadsheets operating within the organisation?	23
52. Are there performance or usability issues that need to be considered when implementing spreadsheet control solutions?	23
53. Who would implement and manage the operation of any spreadsheet solutions?	23
54. Is it as straightforward as installing the software in order to manage the risk or to be compliant?	24
<b>About Protiviti Inc.</b>	<b>25</b>
End-user computing risk management services	25
<b>Contacts</b>	<b>26</b>

# Introduction

Spreadsheets are everywhere. They enable us to quickly and flexibly perform analysis that otherwise would be difficult or time-consuming. As a result, we tend to place undue trust in the integrity of the analysis spreadsheets make.

As spreadsheet users have become more information technology (IT) proficient, their spreadsheets have become more complex. Spreadsheets were never designed to be enterprise-level applications, but the growing use of complex and user-defined functions, lengthy macros and links to other spreadsheets and systems has led to the development of highly complicated applications. In contrast to most other applications of this nature and criticality, spreadsheets rarely are designed and developed by expert users or with controls in mind.

Many companies rely on spreadsheets as a key application that supports operational and financial reporting processes. The purposes of spreadsheets are widespread, from performing complex modelling for trading decisions to accounting reconciliations and calculating employee bonuses.

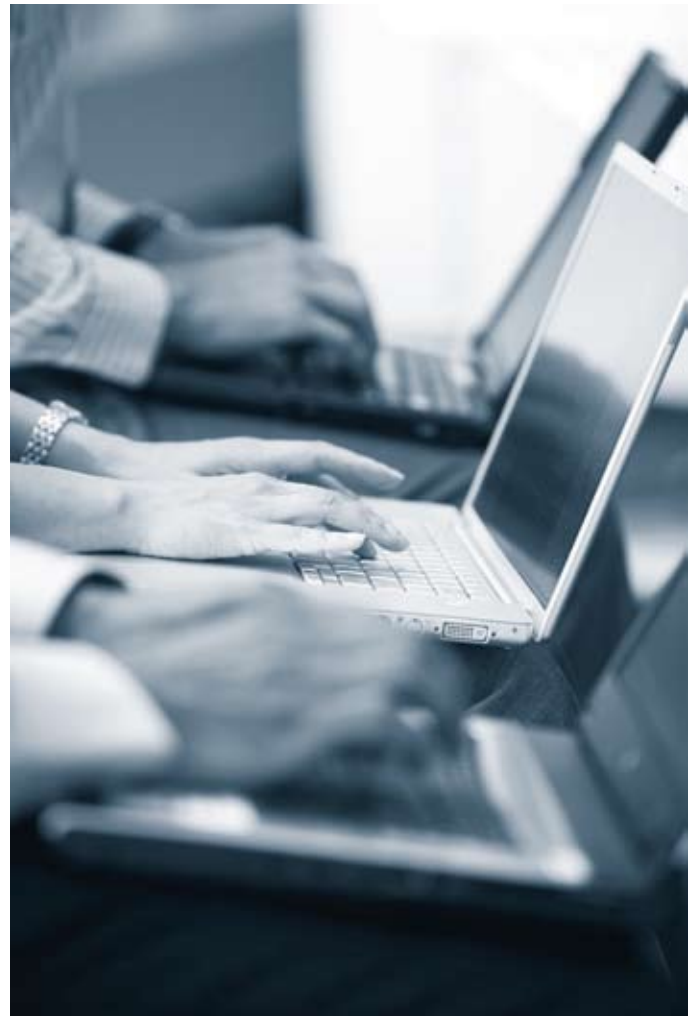
A simple search of your network may surprise you as it will reveal thousands, if not millions, of spreadsheets in use. Do you know who manages them? What is the purpose of these spreadsheets? How reliable are their calculations? Who ensures the results they produce are valid?

The increased regulation and compliance that now impacts spreadsheet control is not surprising given that the past few years have seen numerous multimillion-pound errors and frauds attributed to the use of spreadsheets. We also see companies filing material weaknesses and deficiencies with the Securities and Exchange Commission (SEC) as a result of the lack of controls around their financial reporting spreadsheets.

This regulatory pressure and increasing focus from auditors is forcing organisations to address the issue of spreadsheet risk management, though few really understand what the issue is and what they need to do about it. While guidance exists, much of it is academic, providing little practical value to companies.

This publication is based on Protiviti's extensive experience assisting our clients in this field. Our approach and guidance represents a pragmatic response to spreadsheet risk based on real business need. Although this publication uses the term 'spreadsheet', much of the guidance applies equally to other end-user-developed applications, such as databases and reports. Spreadsheets are the most prevalent of end-user applications, but there are other types growing in numbers that should not be ignored.

**Protiviti**



# An introduction to spreadsheet risk management

## 1. Why are spreadsheets so prevalent today?

Technology is developing rapidly, as are users' expectations about what it should deliver – and when. This impatience poses challenges for IT departments. When the IT department cannot meet users' expectations, they are more likely to explore alternative options.

A spreadsheet is a powerful tool that in many cases is a viable alternative to lengthy software development cycles for users who require results immediately or need to keep ahead of the competition. As a result, spreadsheets are everywhere. They enable users to quickly perform analysis that otherwise would be difficult or time-consuming.

The ability of the user to develop and configure powerful solutions in a spreadsheet environment without appropriate training or awareness is introducing a high degree of spreadsheet-related risk into the corporate environment. This level of risk will grow with the increasing use and complexity of spreadsheets.

The key reasons behind the growing use of spreadsheets include:

- They are flexible and easy to use.
- Immediate results are generated, with potentially very short development periods.
- It is easy to become reasonably proficient in the use of a spreadsheet (though it is less straightforward to become reasonably proficient in their design and development).
- They can be configured to the personal requirements of the user.
- They are readily accessible by nearly all users, as they are usually a standard corporate desktop application.
- Spreadsheets can support the download and analysis of data from core systems.
- Over time, users have become more advanced in their use of spreadsheets.
- Spreadsheet software itself has become increasingly powerful over the years, opening up greater functionality to users.

## 2. What is spreadsheet risk management?

A fundamental problem with spreadsheets is that untrained users tend to place undue trust in the integrity of the analysis that is prepared in them. As users become more IT-literate, the number of spreadsheets in use is increasing, and they are becoming significantly more sophisticated.

Many companies rely on spreadsheets as a key application that supports operational and financial reporting processes. The purposes of such spreadsheets are widespread, from performing complex modelling to make trading decisions, to accounting reconciliations, to calculating employee bonuses.

Spreadsheet risk management helps ensure that the risk presented by spreadsheets is understood and appropriately mitigated.

## 3. Why do spreadsheets present a risk?

Spreadsheets can provide a broad spectrum of solutions to the user. The following table contains some typical examples of spreadsheet uses and how they can go wrong:

Use	What can go wrong
Billing	<p>A major telecom organisation invested millions in core billing systems to support their key revenue earning stream: billing customers for calls made. For certain corporate customers, however, the billing rules, which were often complex, changed from year to year.</p> <p>The billing team concluded that for these corporate customers, it was too difficult for IT to change the systems on a yearly basis. Therefore, flexible spreadsheets were designed that would download data from the core systems and calculate the invoices.</p> <p>The billing rules were too complex for spreadsheet owners to constantly check for possible user errors. As a result, errors were soon identified.</p> <p>While lost revenue was recovered from the relevant corporate customers, the reputational impact on the telecom organisation is difficult to quantify. Had a detailed review of the spreadsheets not been performed, the revenue leakage would have remained undetected.</p>
Reporting	<p>An accounting consolidation package provided a reporting function that could not be configured to support the changing reporting requirements of the finance department.</p> <p>Spreadsheets were built that took the financial reporting information from appropriately controlled Enterprise Resource Planning and consolidation system software, manipulated the data and provided reporting to senior management.</p> <p>Controls around the systems were regularly reviewed and assessed as operating effectively. The spreadsheet was never in scope for the reviews as it was owned within finance by the individuals responsible for reporting.</p> <p>When the spreadsheets were reviewed in detail, a significant error was identified in the calculation of year-end accruals – a result of an error within a number of the calculations performed outside of the system in the spreadsheet.</p> <p>Significant investment had occurred to ensure that systems were appropriately configured and controlled. This investment was entirely undermined by the creation of spreadsheets to produce reports that should have been configured in the core IT systems.</p>

Use	What can go wrong
Pricing	<p>A commodities trading firm priced and managed exposure on its options trading book through a complex spreadsheet that included a coded Monte Carlo algorithm.</p> <p>The spreadsheet was produced by a trader with advanced spreadsheet knowledge. The trader also operated additional manual controls that provided assurance that the spreadsheet was accurately calculating price and exposure levels.</p> <p>When the trader moved to another organisation, the spreadsheet was inherited by a new options trader who was not an advanced user of spreadsheets. This trader made some assumptions about the spreadsheet's operation. Over time, errors were introduced into formulas and exposure levels were tracked inaccurately. Options were incorrectly traded and month-end profit and loss analysis showed a significant loss on the options book.</p> <p>The error was tracked back to inaccuracies within the spreadsheet. The options trader had no knowledge of the errors.</p>
Budgeting	<p>A consulting firm employed basic spreadsheets to price and budget client engagements. The spreadsheets provided analysis that allowed the engagement managers to calculate the hours and level of the team on the engagement. The objective was to ensure that the firm achieved a certain margin on each engagement. The spreadsheets, while relatively simple, had little or no control over the content. Formulas could be changed and pricing tables updated.</p> <p>When errors were accidentally introduced into an engagement budgeting spreadsheet, they did not result in significant financial impact for that particular engagement. However, the error was significantly compounded when the spreadsheet was shared among all the engagement managers and the model was used to price other engagements.</p> <p>Eventually, it was discovered that major engagements had been priced inappropriately and the firm would not achieve its target margin. The lost money was not recoverable from the clients, as fees were part of already-signed contracts.</p>

Use	What can go wrong
Data quality	<p>Many organisations use spreadsheets as a simple tool for capturing data on large projects. A common example of this has been the capturing of data on risk and control for Sarbanes-Oxley projects. Spreadsheets are also often used to track remediation and closure of gaps.</p> <p>Businesses are often left with large numbers of spreadsheets that must be maintained over time. Organisations that have adopted this approach often want to extract information from the templates and use it – for example, to prepare weekly/monthly progress reports.</p> <p>Many organisations that have adopted this approach have found that the production of management information is extremely time-consuming. Furthermore, when the data is consolidated into monthly reports, inconsistencies are often identified. These are typically a combination of timing issues and errors.</p> <p>Another common problem is that there often are multiple users of the spreadsheets. This results in significant version-control issues as the wrong versions are picked up and used or two users attempt to make changes simultaneously, potentially undoing each other's changes.</p> <p>Though the direct consequences of these data quality issues were not significant, the cost of manually producing management information and resolving the quality issues was substantial.</p>

In addition to these examples, a simple Internet search for spreadsheet errors reveals numerous examples, including budgeting errors, financial statement errors, pricing errors, and fraud or bad decision-making as a result of poor information. The financial impact can be significant (many millions of pounds) and the damage to a company's reputation can be even worse.

Some frequently quoted examples include:

"A cut-and-paste error cost TransAlta \$24 million when it underbid an electricity-supply contract."

Source: *The Register*

"Falsely-linked spreadsheets permitted fraud totalling \$700 million at Allied Irish Bank/Allfirst."

Source: *EuSpRIG*

"Kodak's SEC 10-K filing reported a material weakness in its internal controls surrounding the preparation and review of spreadsheets that include new or changed formulas."

Source: *Compliance Week*

As spreadsheet users have become more proficient, their spreadsheets have become more complex. Spreadsheets were never designed to be enterprise-level applications. However, the growing use of complex and user-defined functions, lengthy macros and links to other spreadsheets and systems has led to the development of highly complicated applications.

#### **4. Is the level of risk increasing?**

Yes. Spreadsheets are becoming more complex and users are finding increasingly novel applications for them. User training and awareness is still limited, however. As spreadsheets become more complex, they are more prone to error. As users are perceived to become more IT-literate, more spreadsheets are being used to support critical business processes. A combination of these two factors is significantly increasing the overall risk profile for many organisations. The perceived level of risk is also rising due to growing awareness and understanding of the risk that uncontrolled spreadsheets pose, as well as increased regulatory and audit scrutiny.

#### **5. What about other desktop tools available to users?**

While this document uses the term 'spreadsheet', the issues and approaches outlined could just as easily apply to other desktop tools available to end users. These tools include database software (e.g. Microsoft Access), reporting tools (e.g. Crystal Reports) or any other 'power' tool that can be configured by the end user and depended upon to support operational processes.

End-user-developed databases can be even more risky than spreadsheets, as in many cases the data manipulation is less transparent to the end user. Reporting tools often allow users to develop customised reports which, if the query is configured incorrectly, can result in users inadvertently restricting the data they report.

However, the key difference between spreadsheets and other desktop tools is that spreadsheets are by far the most commonly used, and have by far the broadest end range of users.

The technology solutions referenced later in this guide to support the management of spreadsheets differ from those available for other desktop tools. In certain cases, the solutions have some functionality that can be applied across multiple desktop tools, but this is generally the exception.

#### **6. Why has spreadsheet risk management suddenly become important?**

Spreadsheet risk always has been important. However, as discussed in answers to previous questions, there are indications it is becoming more significant.

The UK's H. M. Customs & Excise, in its *'Methodology for the Audit of Spreadsheet Models'* (2001), said that "the complexity and functionality of spreadsheets has reached levels of sophistication that few could have imagined even five years ago. The consequent threat posed to businesses by such powerful 'end-user' applications, mainly in the hands of untrained users, is immense". This observation has continued to hold true in the years since its publication.

It is also fair to say that recent regulatory compliance initiatives have forced organisations to consider the spreadsheet risk to which they are exposed. In particular, guidance produced in support of the Sarbanes-Oxley Act has advised organisations to specifically consider spreadsheet risk. Regulatory bodies and external audit firms have detected the increasing exposure to spreadsheet risk and are taking action to ensure it is addressed.

#### **7. Do technology solutions exist that can assist with managing spreadsheet risk?**

Yes. The section 'Technology enabling effective spreadsheet risk management' provides more detail about the types of solutions available.

# Executive ownership and governance

## 8. Who is accountable for effective spreadsheet risk management?

Senior management ('the executive') including, but not limited to the board, is ultimately accountable, on behalf of the organisation, for the effective management of all risk, including spreadsheet risk. This executive accountability is usually to the shareholders (where applicable) and the regulatory bodies governing the industry and environment in which the organisation operates.

The executive must understand:

- What is the risk?
- Where does the risk exist?
- How significant is the risk?
- Who is currently dealing with the risk?
- When will this risk be managed to an acceptable level?

Given the ever-increasing dependency on spreadsheets, as well as the external focus on them, the executive is increasingly aware that spreadsheet risk is an area of exposure that should be actively managed. This potentially time-consuming task should leverage many of the risk management processes already in operation, including current compliance efforts.

## 9. What do the major legislative acts have to say about spreadsheets?

The major legislative acts in existence today, namely Sarbanes-Oxley, Companies Act, Turnbull, Basel and MiFID, do not focus specifically on spreadsheet risk. However, effective management of spreadsheet risk is required to satisfy the requirements of each of these regulations.

Legislation tends to provide more generic statements such as, "An effective system of internal control..." (Turnbull). This ensures a broad sweep of requirements that will cover as many scenarios as possible within a diverse commercial environment. Therefore, organisations and the monitoring bodies (e.g. external audit firms, regulatory authorities) are required to interpret the legislation and determine how its requirements should be applied to each organisation.

What has become clear over the last five years is that the regulatory bodies and audit firms are becoming increasingly aware of the potential exposure to spreadsheet risk that can exist in an organisation. In fact, this issue became so significant during the Sarbanes-Oxley compliance peak between 2004 and 2006 that the major audit firms released various papers and guidance to ensure organisations were aware that spreadsheet risk management was an area they would be focusing on specifically. In many organisations, they found that managing spreadsheet risk was an issue for which no one in the organisation was taking accountability.

Spreadsheet risk management is therefore a requirement for all organisations that are subject to these regulations. The only scenario in which this would not apply is when an organisation has no significant business processes supported by spreadsheets.

In fact, the only way an organisation without an effective spreadsheet risk management strategy can be confident it is not exposed to significant risk is to prevent users from having access to the application. This is clearly not a practical solution for most organisations.

## 10. How can the executive define and communicate their spreadsheet risk management requirements?

Typically this is achieved by creating a spreadsheet risk management policy that states what the executive expects from the organisation. Then, the organisation will need to define how it implements the policy in a spreadsheet risk management operating model. This operating model should set out accountability, roles and responsibilities, processes, controls and minimum control standards.

When defining such requirements, the executive should take into account processes in place to ensure compliance with any existing policies. If there is not an effective compliance process in place, it is likely the spreadsheet policy will become another ineffective piece of paper on the pile of existing policies. Further guidance on implementing an effective governance, risk and compliance programme can be found in Protiviti's *Enterprise Risk Management FAQ Guide*.

If clear and regular assurance is provided to the executive on other policies, the executive can be more assured that introducing a spreadsheet risk management policy will be an effective vehicle for ensuring the organisation can begin to effectively manage spreadsheet risk.

## 11. Who should operate spreadsheet risk management processes?

Because the IT department provides the infrastructure and software critical to the operation of the spreadsheets, it is obviously responsible for ensuring that this aspect of the technology is effectively controlled. However, the IT department cannot be held solely responsible for operating risk management processes around individual spreadsheets.

Spreadsheets are designed, implemented, updated, tested (sometimes) and made operational by the owners and users of those spreadsheets. This is why spreadsheets are so prevalent, and this should not change. However, spreadsheet owners should be responsible for operating effective spreadsheet risk management processes.

The executive should define, on behalf of the business, what constitutes effective spreadsheet management processes. The executive also should ensure appropriate monitoring is put in place to ensure compliance with these processes.

It is important that organisations do not let responsibility for spreadsheet risk management fall between the gaps. The business side often considers spreadsheets to be IT's responsibility and removes them from the scope of any risk management work. The same goes for IT professionals, who often consider spreadsheets to be owned by the business side. Clearly, if nobody is taking responsibility for spreadsheet risk management, the executive has a problem.

The organisation can resolve this confusion by defining clear roles and responsibilities within the spreadsheet risk management operating environment.

The IT department may be able to provide solutions to assist with effective spreadsheet risk management. In this scenario, the IT department would become accountable for the effective operation of these solutions; therefore, the responsibility for effective risk management may be shared between the IT department and the spreadsheet owners.

In practice, co-operation between business and IT is critical to the operation of an effective spreadsheet risk management environment.

### **12. Why should we report on spreadsheet risk to senior management and the executive?**

Creating a reporting process that demonstrates an effective spreadsheet risk management process is critical for the following reasons:

- It allows operational management and the executive to understand the key risks to the organisation, the significance of those risks and the work in progress to manage those risks.
- Better transparency of spreadsheet risk management drives better behaviour among operational personnel.
- Demonstration of effective risk management processes is critical for satisfying legislative requirements.

Failing to implement a discrete process for reporting on the effectiveness of the spreadsheet risk management environment is a missed opportunity. Ensuring there is transparency over the effectiveness of the whole operational risk management environment is a goal any organisation should look to achieve.

Many organisations already have some form of operational risk management reporting process in place. In these cases, the critical step is the integration of the spreadsheet risk management processes into the current assessment and reporting approach.

### **13. What should the risk responsibilities of a spreadsheet owner cover?**

The spreadsheet owner should be responsible for the identification and assessment of operational risks that exist in the spreadsheets they own.

In fulfilling these responsibilities, the spreadsheet owner should be provided with guidance on what is expected and given access to the tools necessary to ensure their assessment of risks and controls is consistent with the rest of the organisation.

The spreadsheet owner should be responsible for the identification and operation of appropriate controls that mitigate the risk to an acceptable level. They also should be responsible for accepting spreadsheet risk within defined limits of authority. Limitations on the amount of risk they can accept should be agreed upon with senior management or the executive.

### **14. What should be the role of the IT department?**

It has been emphasised that the spreadsheet owners are responsible for controlling the risks associated with their spreadsheets.

However, there is an assumption that the IT infrastructure relied upon by the spreadsheet owners is available and secure. This is the responsibility of the IT department. A lack of control over this infrastructure typically has an impact on the availability or security of spreadsheets (as well as a pervasive impact across other technology within the organisation).

When assessing the risks associated with a spreadsheet, the spreadsheet owner might choose to rely on the controls operated by the IT department. For example, a spreadsheet may be needed every day to process key transactions. The availability of the spreadsheet is therefore critical, and the spreadsheet owner will wish to establish that the spreadsheet will be available and can be recovered in the event of any problems. The owner will have to establish the effectiveness of these controls through interaction with the IT department.

Another example involves access to the spreadsheet. The spreadsheet owner may determine that the spreadsheet should be restricted to certain individuals. Therefore, IT may need to set up a storage location that has restricted access and ensure these restrictions are maintained unless further access has been authorised by the spreadsheet owner.

In both of the above examples, IT implements the required controls. However, these controls have been defined by the spreadsheet owner, who must assess the adequacy of these controls against the risks he is seeking to address.

### **15. What should be the role of operational risk departments?**

Operational risk departments exist within many organisations. Typically, mature operational risk management frameworks already have been implemented and processes around these frameworks are well established and operating effectively. A risk management framework cannot be mature, however, if it does not consider all the risk to which the organisation is exposed.

Therefore, the challenge for the operational risk department is to ensure the risk framework encompasses and ensures effective spreadsheet risk management. One option is to incorporate the spreadsheet risk management policy into the overall risk framework. Doing so allows spreadsheet risk to be considered within an existing risk management governance structure, rather than considering spreadsheet risk management as an independent activity.

### **16. What should be the role of internal audit?**

In many organisations, it is the responsibility of internal audit to provide a level of independent assurance to the executive that risk within the organisation is being managed effectively. Internal audit should focus on the spreadsheet risk management controls in operation. Typically, in organisations that are starting to review the effectiveness of spreadsheet risk management, the controls will be ineffective, necessitating gap analysis and remediation. If there are no overarching controls in operation, internal audit often can help get these issues on the executive's agenda.

Internal audit should in general avoid doing detailed testing of individual spreadsheets for integrity. Performing reviews of individual spreadsheets is likely to focus the organisation on resolving issues within individual spreadsheets rather than addressing the root cause of the problem: ineffective spreadsheet risk management controls. One-time integrity testing of individual spreadsheets is important to ensure they are operating as intended, but this testing does not necessarily need to be performed by internal audit.

# Creating a library of critical spreadsheets

## 17. How do we measure risk?

Spreadsheet criticality is defined as the likely impact to the organisation of an error occurring in the spreadsheet. Ideally, any spreadsheet risk should be evaluated in terms of its likely financial impact. However, a financial quantification is often too complex to implement during the initial assessment of critical spreadsheets. Therefore, organisations have employed a more general scale for estimating likely impact. An example is provided below:

- **Low:** No key business decisions are made based on the information contained within the spreadsheet. Errors that occur would be of embarrassment or hindrance to those directly associated with the spreadsheet, but would have no real long-term impact on the business.
- **Medium:** An error in the spreadsheet or a delay in preparing the spreadsheet may result in significant loss to the business. Information contained in the spreadsheet may be sensitive and employees could exploit the information if they had access to it.
- **High:** An error in the spreadsheet or a delay in preparing the spreadsheet may result in a material loss to the business. Information contained in the spreadsheet is highly sensitive and inappropriate disclosure could be exploited by markets or competitors, or could be in breach of legislation (e.g. the UK Data Protection Act or the US Health Insurance Portability and Accountability Act or Gramm-Leach-Bliley Act).

To determine which spreadsheets pose the highest risk within the organisation, the inherent risk of a spreadsheet must be assessed. Inherent risk is defined as: 'The risk to an organisation in the absence of any actions management might take to alter either the risk's probability or impact' (Institute of Internal Auditors). A spreadsheet's inherent risk is, therefore, a combination of its criticality (impact) to the organisation and the inherent likelihood of error in the spreadsheet, which is derived from a combination of the complexity and the design of the spreadsheet.

To determine the complexity of a spreadsheet, the following key characteristics should be reviewed:

- Spreadsheet size.
- Complexity of formulas.
- Volume of linkages to other cells, tabs and spreadsheets.
- Volume of data.
- Existence of Visual Basic code.

This can be a time-consuming process for large spreadsheets, but software tools can automatically scan spreadsheet files and produce a score based on a predefined scale of complexity.

However, the likelihood of error involves spreadsheet design as well as complexity. Assessing design involves reviewing each spreadsheet in turn and identifying characteristics of bad design that could increase a spreadsheet's likelihood of error. Examples of bad design include hard-coding of numbers or assumptions into formulas and inconsistent or overwritten formulas within a column or row, which result in a higher likelihood of error.

Calculating the inherent risk of spreadsheets allows the organisation to focus any subsequent effort on those spreadsheets with the highest risk. An effective way to illustrate the spreadsheet risk profile is the use of a risk map. Figure 1 shows a simple example of a risk map:

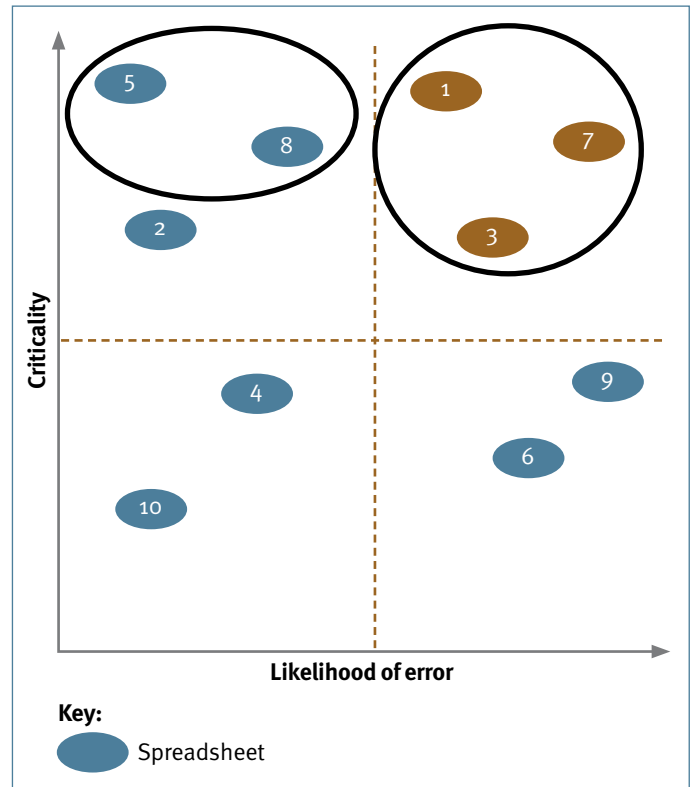


Figure 1: Simple example of a spreadsheet risk map

The business should focus most of its efforts on the spreadsheets with a high criticality and high likelihood of error, as shown in brown in Figure 1. However, it is important that the organisation does not ignore spreadsheets with low likelihood of error but high criticality. Some of these spreadsheets may need to be controlled, as the occurrence of an error could have a significant impact on the organisation. Such spreadsheets are shown circled in the top left of Figure 1.

Even the simplest spreadsheets often contain errors, as is illustrated by the budgeting example in Question 3. In our experience, simple spreadsheets are often subject to very limited or no testing and as a result, are often more prone to significant errors than complex spreadsheets, which may be more thoroughly tested.

### 18. How do we start to identify the potentially critical spreadsheets?

There are a number of ways to start the process of identifying the critical spreadsheets, including:

- Automated scanning tools.
- Questionnaires.
- Process documentation (where available).
- Interviews or workshops.

The best way to start is usually by performing an automated scan of the network to identify potential spreadsheets. This will quickly identify any potentially complex spreadsheets in use as well as parts of the business most reliant on spreadsheets.

However, the most effective way of identifying critical spreadsheets is to hold discussions with key individuals, process owners and department heads. Any initiative to implement an effective spreadsheet risk management model should start with the areas perceived to be the most dependent on spreadsheets, have significant operational importance, or have had previous spreadsheet incidents.

When discussing the spreadsheets individuals are dependent on, it is often useful to start from the premise that dependent spreadsheets are those that, if deleted, would either take too long to re-create (in some cases, just one hour redeveloping a spreadsheet can be too long) or could not be re-created at all. The output of an automated scan also can be helpful when holding these discussions to ensure all complex spreadsheets currently in use are discussed.

The next stage is to identify the spreadsheets that, if inaccurate, would have a negative impact on the organisation. This can be a challenge, as the individual will want to consider other controls in operation that mitigate the risk. However, it is important that the individual focuses on potential financial impact in the context of inherent risk (i.e. without controls). This is so that the organisation can ensure that, when the assessment of controls is performed later in the process, either the controls fully mitigate the inherent risk or the residual risk is understood and accepted.

### 19. Which parts of the organisation can have the greatest dependency on critical spreadsheets?

The functions/divisions that are most dependent will vary by organisation. There are, however, some key risk indicators (KRIs) that can be used to quickly prioritise efforts on parts of the organisation that most likely have an increased dependency on spreadsheets. These indicators include:

- A high volume of spreadsheets, rather than formal applications, are known to support critical processes.
- Spreadsheets are used to manipulate data prior to input into an application, or after output.
- Known incidents, including error or actual financial losses, have occurred as a result of spreadsheets.
- Spreadsheets are used as interfaces between systems.
- Calculations are performed in spreadsheets because they are too complex to be performed in systems.
- Processes or transactions change to meet market requirements (this often indicates that core applications cannot support changing business requirements as well as spreadsheets can).

In addition, finance and 'front office' functions are often users of critical spreadsheets due to the nature of the roles they perform.

### 20. How can we ensure that we identify all potentially critical spreadsheets?

It is not possible to be completely sure that all critical spreadsheets have been identified, but an organisation can scan the file servers for all spreadsheet files. Typical searches can reveal millions of spreadsheets, many old and obsolete. Simple analysis can help focus on the potentially critical spreadsheets. In considering any such analysis, organisations should be aware that cost-effective tools exist that automate a large part of the work and greatly decrease the time and effort required.

Analysis should be performed on the 'last modified' date to identify spreadsheets that have been active in the last six months (or 12 months, depending on the organisation's risk appetite). Analysis could then focus on the spreadsheets that exceed a certain size (larger spreadsheets are typically more complex and therefore often have a higher inherent risk). It is also worth trying to identify whether multiple spreadsheets are actually different versions of the same spreadsheet, where a user regularly saves the spreadsheet with a different date or version number. Many of the leading automated scanning tools automatically take these factors into account.

For discussions with users regarding their critical spreadsheets, it is useful as a completeness check to have a list of spreadsheets the users are currently recorded as owning and have recently used. During these discussions, it is often discovered that some spreadsheets are being used as workarounds for systems or reports that do not meet the needs of the business. Information regarding workarounds for ineffective systems is worth capturing, as it can be fed into the change/enhancement processes for these systems.

The other common type of critical spreadsheet is one that forms part of the control environment around the core business process (e.g. a spreadsheet containing control totals, checks or reconciliations). These spreadsheets are important as they are being relied upon to identify potential errors in these core business processes.

Simple spreadsheets used to record personal information should not be overlooked. These spreadsheets are not likely to be deemed critical to the organisation, but access may need to be tightly controlled in order to meet privacy standards in many countries.

### **21. What about spreadsheets that have links to other spreadsheets?**

The organisation needs to ensure that any dependencies between spreadsheets are identified and recorded. (It is possible to link spreadsheets together by referencing cells in another spreadsheet or through Visual Basic code created in a spreadsheet.)

If a spreadsheet is critical, but also dependent on the accuracy of information contained in another spreadsheet, the organisation needs to record the spreadsheet that is providing input. Discussions with individuals often will identify only the top-level spreadsheet. However, this top level may be dependent upon a network of sub-spreadsheets. It is not uncommon to observe multiple layers of linked spreadsheets.

Tools exist that automatically identify any spreadsheets that feed information to a selected spreadsheet; they also can search Visual Basic code for key function names. This is essentially a completeness check, but a very important one, in that it can ensure all critical spreadsheets have been recorded. Generally, a spreadsheet that provides information to a separate critical spreadsheet will itself be critical. The information collated can be used to create a map or diagram that is useful to illustrate the dependencies and data architecture.

# Implementing a spreadsheet control framework

## 22. What is a spreadsheet control framework and why is it important?

A spreadsheet control framework is the structure an organisation implements to define the spreadsheet risks and the associated controls that should be considered.

A control framework:

- Ensures minimum standards are clearly documented and consistently communicated.
- Identifies standard risks and controls that critical spreadsheets in the organisation can be measured against.
- Provides the opportunity to re-evaluate the minimum standards and ensure amendments to executive or legislative requirements can be incorporated centrally into the framework and rolled out across the organisation.

The effective implementation of a spreadsheet control framework should be assessed through management assurance processes or through independent evaluation (e.g. by internal audit).

## 23. What are the typical key components of a spreadsheet control framework?

The control framework should identify the key organisation-level risks that spreadsheets are required to be assessed against, such as financial, reputational and regulatory. Control objectives should be defined against each of these high-level risks.

Given the similarities between spreadsheet development and application development, it is appropriate to leverage an industry-recognised IT control framework. By using existing frameworks, the organisation can select the control objectives that apply, but also provide a level of assurance that all possible areas of risk and control have been considered. One framework to consider using is Control Objectives for IT, or CoBIT.

The reason for having control objectives is that spreadsheet owners can assess each of the high-level risks for their spreadsheets and then assess how the current controls achieve the associated control objectives.

Some of the control objectives may be deemed mandatory or key, and should be defined clearly in the spreadsheet policy (e.g. spreadsheet security). For other control objectives not classified as mandatory, the ultimate decision about which objectives apply may be left to the spreadsheet owner. The controls objectives that apply will depend on the level of risk and the criticality of the spreadsheet.

A typical set of controls that could be incorporated into the framework are suggested below. The extent to which these controls must be applied will vary on a case-by-case basis:

- **Access control:** Defining and maintaining appropriate user access rights and restrictions, including segregation of duties where applicable.
- **Backups:** Backup of spreadsheets and data to ensure continuity and availability.
- **Change control:** Controlling changes that are made to the spreadsheet, including adequate testing and documentation of changes.
- **Data input validation:** Ensuring completeness and accuracy of data inputs.
- **Data integrity and security:** Preventing unauthorised modification of the spreadsheet and protecting sensitive cells from accidental change or deliberate manipulation.
- **Development control:** Controlling the development process, testing and deployment of new spreadsheets.
- **Documentation:** Appropriate documentation maintained to describe the owner, business objectives, functions, change history, assumptions, external links and any other relevant information. This would extend to documenting macros or Visual Basic code if applicable.
- **Independent review:** Documented independent review of spreadsheet logic and changes.
- **Version control:** Ensuring that only the current version of the spreadsheet is used, and specific previous versions can be retrieved or re-created if required.

The IT Governance Institute, in its *'IT Control Objectives for Sarbanes-Oxley, 2nd Edition'*, provides a set of illustrative key controls for end-user computing, which includes spreadsheets. These controls consist of:

- Existence of and adherence to policies and procedures.
- Documentation and regular integrity review of end-user computing applications.
- Backup and secure storage of applications and data.
- Security to prevent unauthorised access.
- Independent verification to ensure completeness and accuracy of inputs, processing and outputs.

The guide also provides a sample approach for spreadsheets, consisting of the following three stages:

- Create an inventory of spreadsheets involved in the financial reporting process.
- Perform a risk assessment (impact and likelihood) of financial statement error.
- Implement and assess spreadsheet controls.

Although this approach is designed for Sarbanes-Oxley, it is consistent with Protiviti's approach to spreadsheet risk management, which can be applied regardless of risk management objectives and nature of spreadsheet usage.

#### **24. When is a spreadsheet not fit for purpose?**

In certain scenarios spreadsheets can be too complex, in which case the organisation should consider migration of the spreadsheet into a structured application controlled by the IT department.

Example scenarios in which this option should be considered include:

- The spreadsheet contains master data used to feed calculations and reports.
- The spreadsheet makes use of a large amount of Visual Basic code.
- There are multiple users of the same spreadsheet.
- The spreadsheet is used as an interface between two systems.
- The spreadsheet is slow and often requires regular restarting.

Transitioning the spreadsheet into a more formal application development environment will significantly reduce the risk. The cost/benefit of this action will need to be assessed. While the overall risk profile is reduced, there may be a significant cost associated with the development and ongoing maintenance of such an application.

# Assessing spreadsheet controls and current risk exposure

## 25. Do we need to assess the controls in operation across all our spreadsheets?

It is not usually necessary to assess controls across all spreadsheets in use. However, the extent to which testing is required will depend on the level of risk the organisation is willing to accept. Typically, spreadsheets with a low level of inherent risk (see Question 17 for more information on risk assessment approaches) are generally not incorporated into a formal spreadsheet risk management model. For these lower-risk spreadsheets, we recommend that spreadsheet owners are made aware of their responsibilities toward spreadsheet risk management, but that the organisation does not require them to perform formal risk and control assessments on their spreadsheets.

## 26. How do we consistently assess controls across spreadsheets?

Consistent spreadsheet control assessment is facilitated by having an effective spreadsheet control framework against which each spreadsheet risk can be assessed. Further guidance on the key requirements of a spreadsheet control framework is provided in response to Question 23. Key aspects of control that need to be considered include: design standards, change management controls, baseline integrity testing performed, documentation retained, access controls and controls over backup.

Key aspects of the overall control environment are likely to be dependent on IT. In particular, IT is likely to be responsible for general controls over access to the network and backup of the network. The assessment of these controls should be performed centrally and reflected in the spreadsheet risk management policy and guidelines.

However, the spreadsheet owner will still need to take responsibility for defining the specific access rights for the spreadsheet. The spreadsheet owner also will need to assess whether the service levels offered by IT and the standard backup/restore processes meet the requirements of the business.

Figure 2 shows a typical split between individual spreadsheet testing and pervasive IT testing. The use of technical management solutions can increase the ability to pervasively or centrally test spreadsheet controls (see the section ‘Technology enabling effective spreadsheet risk management’).

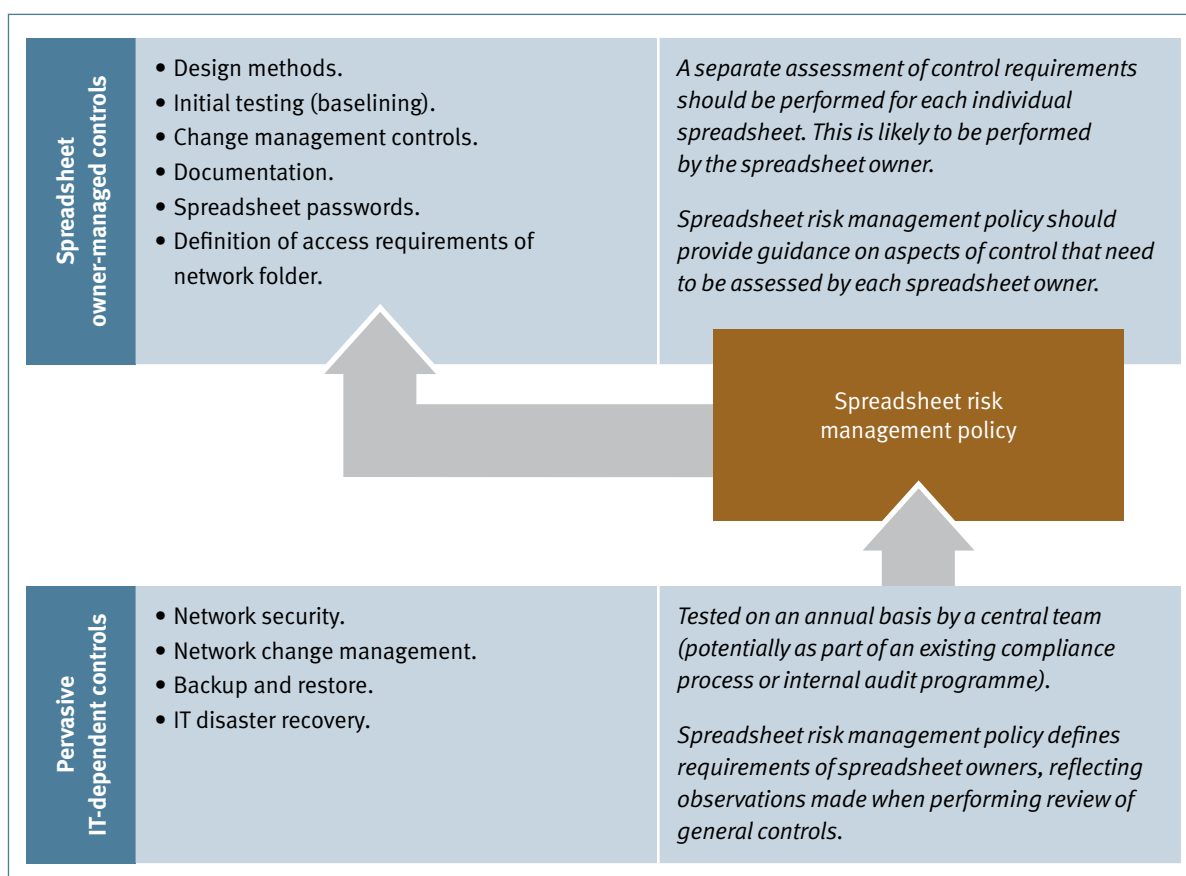


Figure 2

The organisation must ensure the assessments are performed by a person with the appropriate skills. If assessment is done by the spreadsheet owners, it is essential that they consistently and effectively assess the controls in operation around their spreadsheets. Many successful projects to implement a spreadsheet risk management framework have employed a central team of experts to provide guidance, training and review on the assessments performed by individual spreadsheet owners.

#### 27. How do we assess whether the controls are effective?

The first step of any assessment is to ensure the controls in operation achieve the minimum control standards defined in the spreadsheet control framework. Having achieved compliance with the minimum control standards, consideration should be given to any other controls that have been implemented. The identification and assessment of controls should use the spreadsheet control framework to ensure the assessment considers all risks and controls and is performed consistently across the organisation.

The next step is to understand the level of residual risk the organisation is exposed to with the controls currently in operation. Residual risk is an assessment of the expected impact and likelihood of error after all risk-related actions have been implemented (e.g. controls or transfer of risk). The residual risk can be determined by considering both the impact of the spreadsheet to the organisation and the likelihood of error.

**Impact:** The spreadsheet owner will need to assess the potential financial impact or consequence of an error arising in the spreadsheet over the next 12 months – hence, the criticality to the organisation. If there are other controls in place that would limit the potential impact – for example, reconciliations that would detect an error – these should be taken into account, whether or not they are independent of the spreadsheet.

**Likelihood of error:** Determined by a combination of the complexity and design quality of the spreadsheet. See the response to Question 17 for further information.

If the calculated residual risk is above that acceptable to the organisation, the controls are inadequate. Then, remediation activities will need to be instigated to improve controls or reduce the spreadsheet's likelihood of error – for example, through redevelopment of the spreadsheet.

#### 28. Can different approaches be taken to resolve any control issues?

There are many different approaches that can be adopted to reduce residual risk to an acceptable level. The spreadsheet risk management framework should provide guidance and provide examples. A prescriptive approach rarely works. The spreadsheet owner will need to assess the potential risk and the control objectives, and then put in place appropriate controls.

By way of an example, any spreadsheet risk management policy is likely to state that access to the spreadsheet should be restricted to appropriate users. One approach may be to add a password to the file, utilising the basic security features of Excel. This provides only a basic level of control as passwords are shared and rarely changed and repeat attempts are allowed.

Another approach (potentially additional to the Excel password) is to set up a directory on the network and grant access to a defined list of users. This should provide a higher level of control, as user accounts are managed centrally and better password standards can be applied. However, under this model all users with access to the spreadsheet do have the same level of access.

Another option is to make use of spreadsheet control software (see the section 'Technology enabling effective spreadsheet risk management'). Such tools can provide greater flexibility, allowing user- or role-based access and segregation of duties in the spreadsheet to be enforced. These tools also provide an audit trail of actions users have performed.

The spreadsheet owner will need to decide what level of control is required, taking into account any requirements of the spreadsheet risk management policy. A basic password may be adequate for some spreadsheets that do not contain sensitive data and only have a few users. This will not, however, be sufficient in many cases.

### **29. How can we identify common control issues across the organisation?**

One of the benefits of implementing a consistent spreadsheet control environment across the organisation is that it is easier to identify common control issues. To gain this benefit, controls identified should be recorded against control objectives within the framework. The same should be done for any planned actions that are raised to reduce residual risk to an acceptable level. By linking actions to control objectives, the organisation is able to analyse where significant control gaps exist.

The actions typically will be tactical solutions implemented locally within the organisation. At this stage there is an opportunity for the organisation to review these tactical solutions and determine if there is a more strategic solution that would ultimately be more cost-effective to the organisation as a whole.

### **30. How do we ensure that control issues are resolved and closed within an acceptable timeframe?**

For every control issue or deficiency identified as part of the spreadsheet review, action plans and responses should be developed and documented. Action owners also should be assigned with responsibility for ensuring that actions are delivered by the agreed close date. When the action is closed, the risk should be re-evaluated and a revised residual risk level recorded.

A process needs to be put in place to ensure all actions are resolved on a timely basis. This will be most effective when it forms part of the existing issues tracking/reporting system monitored by an appropriate group (e.g. internal audit, compliance, risk).

A clear escalation policy should be defined to assist action owners where support is required and ensure they are motivated to resolve issues on a timely basis. Long-overdue actions should be escalated through the chain of command. There are instances where slippage is attributable to unavoidable operational reasons, but too often these are used to justify not addressing known control issues. Ironically, it is often the case that control issues are the root cause of continued operational incidents.

### **31. Who is responsible for accepting the residual risk that exists within a spreadsheet?**

A process needs to be implemented to ensure that appropriately qualified and authorised employees are accepting risk on behalf of the organisation. Spreadsheet owners may be accepting significant risk associated with their spreadsheets rather than implementing appropriate action plans.

Defining levels of risk authority means that any residual risk above defined levels will need to be escalated to a higher-level authority within the organisation; for example, a residual risk level of £100,000 or below can be accepted by the spreadsheet owners, while a risk level of more than £100,000 and less than £500,000 needs to be escalated to the department head.

There is a danger that this approach will encourage spreadsheet owners to underestimate the level of risk associated with their spreadsheets. Therefore, it is important that spreadsheet risk evaluations are reassessed by skilled professionals – through the involvement of internal audit, for example.

An option that has worked for some organisations is defining and applying authority limits based on the inherent risk, not the residual risk. This should ensure that any high-risk spreadsheet is subject to some form of independent review and sign-off. See the response to Question 17 for more information on assessing inherent risk.

There is also an argument for emphasising to spreadsheet owners that if they significantly underestimate that risk and incidents associated with their spreadsheet occur, that underestimation will be considered a major failing in their personal risk management performance as well as that of their department. Any effective compliance programme should look for evidence of this type of behaviour.

# Gaining assurance over critical spreadsheets

## 32. How can the organisation ensure that spreadsheet owners are appropriately managing spreadsheet risk?

There are a number of options the organisation can employ.

The first focuses on individual spreadsheets. Through the assessment of inherent risk, the organisation is able to list its most critical spreadsheets. For each of the most critical spreadsheets, the organisation should consider an independent review of all aspects of the spreadsheet owner's responsibilities. This should include the operation of key controls for the spreadsheet and a review of the risk assessments performed by the spreadsheet owner. Independent review should be performed by experienced professionals. Such a review could be performed by a specialist team, internal audit or a third-party organisation.

An alternative approach is identifying a basic set of key controls from the spreadsheet control framework that should be implemented in all spreadsheets. Some form of testing then will be performed, whether as part of a self-assessment process or as part of an independent review. This approach provides a level of assurance to the executive that at least the minimum control standards are being achieved across all key spreadsheets. This approach does not necessarily look at the responsibilities of the spreadsheet owner, but focuses on the controls in operation. This tends to be the approach taken by most organisations as they improve their overall spreadsheet risk management environment.

Other potential options are considered in response to Question 37.

## 33. Where controls have been deficient, how can we rely on the integrity of the spreadsheet?

This can be one of the biggest issues within spreadsheet risk management. When a spreadsheet's controls have been evaluated as ineffective, the organisation cannot rely on the integrity of that spreadsheet until it has been tested and an adequate control environment established.

The introduction of controls alone will not mean that a spreadsheet is complete and accurate. Implementing controls will reduce the risk that new errors are introduced going forward. However, if the spreadsheet is inaccurate when the controls are first implemented, it will remain inaccurate. Therefore testing is required to obtain assurance that critical spreadsheets have integrity.

The testing of a spreadsheet can appear daunting or even impossible. However, there are techniques that can be employed to provide a reasonable level of assurance at minimum cost.

Before these techniques are discussed, it is worth noting that any spreadsheet containing Visual Basic code or macros should be subject to more formal application development testing of the code.

Spreadsheet testing/auditing tools (see section 'Technology enabling effective spreadsheet risk management') are available that will help to perform analysis of formulas, spreadsheet links and data. The output from these tools should be analysed and any anomalies investigated with the spreadsheet owner. Although these tools cannot completely automate the testing of spreadsheets, they make the process considerably more efficient and facilitate tests that would be impractical to perform manually.

For the most critical spreadsheets, this mechanical process will not be sufficient. Other options include performing sensitivity testing, changing key parameters and predicting the impact of these changes on the spreadsheet. This can be an effective final step to check that the spreadsheet appears to be functioning correctly. Sensitivity analysis alone, however, will not be sufficient to identify all potential errors.

There also may be significant benefit to building check totals into the spreadsheet to identify potential issues early. Ultimately, the spreadsheet owner must confirm that someone has checked the accuracy of the spreadsheet and that it is operating as expected.

## 34. Is it possible to rely on the spreadsheet risk management process to provide assurance over the critical spreadsheets?

An effective internal control environment reduces the likelihood that errors or irregularities will occur and remain undetected, but it does not eliminate that possibility. Similarly, well-defined spreadsheet risk management processes will significantly reduce – but not eliminate – an organisation's exposure to spreadsheet risk. For many organisations, adherence to a well-defined spreadsheet risk management policy will reduce the risk to an acceptable level, as well as helping to satisfy regulatory requirements. (Note, however, that these requirements also may necessitate an assurance process to ensure the spreadsheet risk management process is operating as defined. Further guidance is provided in response to Question 32.)

### **35. How often should spreadsheets or the spreadsheet control environment be evaluated?**

The spreadsheet risk management process should be subject to the same assurance approach as other operational risk management processes. Many organisations will look to gain annual assurance over the design and operating effectiveness of the spreadsheet risk management operating model.

However, for many organisations the implementation of a spreadsheet risk management policy represents a significant change. As a result, for areas of high risk, areas where a high volume of complex spreadsheets have been identified or areas where a high volume of control deficiencies have been identified in the past, the organisation should consider increasing the frequency of management assurance testing until the new processes have been embraced by the business.

### **36. Should internal audit be relied on to provide assurance on behalf of the business?**

It is the responsibility of operational management to ensure the organisation has appropriate controls in place that are operating effectively. The operational management team should therefore ensure that adequate assurance processes are in place.

Internal audit may assist management in providing this assurance. The role internal audit plays is entirely dependent on the relationship the internal audit department has with the operational side of the business as well as the priorities of the audit committee.

If internal audit does support operational management by performing an audit or review, it remains the responsibility of operational management to ensure the scope of their review is sufficient to provide the desired level of assurance.

# Spreadsheet risk indicators and reporting

## 37. What other forms of assurance can we rely upon rather than periodic controls assessments?

Many organisations have revisited their regulatory compliance approach to place increased reliance on high-level monitoring controls to reduce their cost of compliance. Technical solutions for managing spreadsheets (as discussed in the section ‘Technology enabling effective spreadsheet risk management’) can provide a method for implementing equivalent monitoring controls around spreadsheets.

Implementing a monitoring tool is not an alternative to implementing an effective spreadsheet risk management framework. Furthermore, before relying on a monitoring tool, it is necessary to perform testing to gain a level of assurance that the spreadsheets are in compliance with policy and free from material errors. Only then can the benefit be gained from implementing a technical solution to detect and notify when changes are made that may or do breach the policy.

This provides much greater assurance than manual assessments because sampling is not required. Consequently, resources can be devoted to ensuring the policy and control framework is appropriate, rather than to performing controls testing.

## 38. Are there generally accepted key indicators of spreadsheet risk or measures that should be applied?

There is no generally accepted set of key risk indicators (KRIs) or internationally recognised standard.

Defining KRIs is about defining a set of measurable parameters that will provide an indication of an increased/increasing level of spreadsheet risk in the area. The organisation should consider having key operational departments report these statistics to management on a regular (e.g. monthly) basis.

The objective of the indicators is to provide a more frequent notification than controls assessments of a potentially increasing exposure to spreadsheet risk as a result of changes to the way spreadsheets are being used to support the business. Where departments have an increasing trend, this could trigger specific work to be performed within the department to ensure that spreadsheet risk continues to be managed effectively.

The focus should be on identifying two or three parameters that can be easily reported but directly monitor spreadsheet risk in the organisation. Some examples of indicators that have been used at other organisations are listed below. Where an indicator uses terms such as ‘critical’ or ‘complex’, the organisations themselves must define at what level these terms become applicable:

- Number of ‘critical’ spreadsheets operated in the department.
- Number of ‘complex’ spreadsheets operated in the department.
- Aggregate inherent risk of all operational spreadsheets.
- Aggregate residual risk of all operational spreadsheets.
- Volume of spreadsheet risk action plans.
- Volume of overdue spreadsheet risk action plans.

The list above is by no means complete. However, it does provide an indication of the type of indicators that the business should be looking to track. It is important that the indicators are simple to measure and easy to produce by a department once effective spreadsheet risk management processes are in operation. Some spreadsheet risk management tools – particularly those designed to perform an automated scan and risk assessment – can be helpful when looking to track some of these indicators.

## 39. What information is provided to the executive/risk committees regarding spreadsheet risk?

Spreadsheet risk should be a single aspect of a much broader operational risk reporting structure. It is important that any information provided to the executive is incorporated into the existing risk reporting processes. This ensures that spreadsheet risk can be assessed in the context of other operational risks that the organisation is exposed to, and prioritised accordingly. The nature and extent of information reported will ultimately be driven by the level of residual risk, when considered alongside other key risk areas the business is seeking to manage.

It is also important that the organisation can demonstrate that in the event significant spreadsheet related issues arise, there are processes in place to ensure that these issues are brought to the attention of the relevant individuals, and appropriate management response actions are in place and prioritised.

Typically an executive will want to know:

- What is the risk?
- Where does the risk exist?
- How significant is the risk?
- Who is currently dealing with the risk?
- When will this risk be managed to an acceptable level?

Note that the above questions could have come from a much more generic approach to operational risk management. Spreadsheet risk also can be aggregated with other types of operational risk to provide an overall risk exposure measure for operational processes, departments, and so on.

The provision of this information also ensures that the executive is fully briefed and in a position to answer questions by external auditors and regulatory bodies.

Further guidance on implementing an enterprise wide risk management process can be found in Protiviti's *Guide to Enterprise Risk Management*, available separately.

#### **40. How can we ensure management and spreadsheet owners take on more accountability for the risk associated with the spreadsheets that they own?**

An effective way of embedding spreadsheet risk management processes is to implement some form of certification process, which also helps to ensure that spreadsheet risk owners take on more accountability. One approach is to ask the individuals accountable for effective risk and control management to confirm the accuracy of the spreadsheets they operate and that all risk and control assessments associated with the spreadsheet are complete and accurate. This can be further enhanced by requiring the individuals to confirm the level of residual risk arising from these assessments.

Having spreadsheet owners assess control effectiveness on a periodic (e.g. quarterly) basis ensures they start to actively own their risk and control assessments and are responsible for maintaining them on a regular basis. It also presents an opportunity for the spreadsheet owner to highlight issues and obtain support in resolving them. From a management perspective, the fact that individuals within the organisation are personally accountable for signing off on this quarterly review provides a certain level of comfort that their spreadsheet risk is managed. Using self-assessment technology can significantly reduce the management's overhead for such a process.

A few organisations have introduced risk management performance into employee contracts, with individuals measured on how effectively they deliver on their risk management responsibilities. However, this can be difficult to implement in many organisations, and most spreadsheet owners will overstate the importance of spreadsheet risk management given their other responsibilities.

#### **41. How can we ensure that spreadsheet risk is incorporated into our current regulatory reporting processes?**

The effective management of spreadsheet risk is already implied in most of the existing regulatory reporting requirements. If spreadsheets are used widely and ultimately relied upon by the business, it is not possible to conclude on the effectiveness of internal controls without considering the effectiveness of spreadsheet risk management controls. Consider whether and how spreadsheet risk has been assessed in the past when the organisation has attested to the requirements of external bodies. Is the organisation comfortable that it has appropriately assessed spreadsheet risk when making these attestations?

If spreadsheet risk has not been formally evaluated in the past, it does not necessarily mean that the organisation has misrepresented its position. It simply means that greater transparency is required around the organisation's conclusions about the effectiveness of spreadsheet risk management.

Organisations need to ensure that spreadsheet risk is considered when making any future statement to regulatory bodies, and it is essential for the executive to understand that spreadsheet risk is actively managed when signing off on any attestation statement. If an organisation has implemented an effective spreadsheet risk management framework and has obtained assurance that this framework is operating effectively, the business will be well placed to reach a conclusion. Essentially, the organisation is required to provide assurance to the executive that the spreadsheet risk policy has been effectively implemented throughout the organisation and that existing issues have been identified and are being actively managed.

# Training and awareness

## **42. Making spreadsheet owners aware of the potential risk is difficult. Are there any tried and tested approaches?**

Increasing spreadsheet risk awareness can be challenging because spreadsheets are typically used by many people within the organisation.

Basic awareness training should be provided, covering the minimum control standards and illustrating some best-practice techniques. It also should provide individuals with guidance on where to go for further information (such as an online resource or a spreadsheet support team). Critically, they should be educated on key indicators that imply significant inherent risk within the spreadsheets they operate, and know whom to contact when these indicators are present.

Users should be provided with regular reminders of the key issues and of their responsibilities. Simply providing some initial training and posting a standard on the intranet is unlikely to achieve the desired level of accountability.

An effective process is to integrate the awareness training into the HR joiner's process. In doing so, all new joiners to the organisation are provided with the training. Training current employees, however, remains a challenge. There are many different approaches to educating a high volume of people, such as those used for internal communications, health and safety awareness and fire drills.

Where critical spreadsheets have been identified, a more formal training programme will be necessary. An alternative to training that has worked well for many organisations is providing a central support team to walk the spreadsheet owner through the process. This is not only more effective than classroom training, but also helps the business achieve consistency in implementation of the spreadsheet risk management framework.

## **43. Are there differing levels of training required for spreadsheet owners?**

This varies and will depend on the individual spreadsheet owners. Spreadsheet owners should have the option to request additional training on spreadsheet development techniques. These typically would be standard spreadsheet training courses that cover more effective use of spreadsheets.

However, specific training on spreadsheet risk management processes will need to be provided to users who own and operate spreadsheets with an increased level of inherent risk. It is also a good idea to review those individuals requesting spreadsheet development training, as this often implies they have a higher dependency on spreadsheets and wish to develop more effective (and probably more complex) solutions. This training should provide guidance on evaluating spreadsheet risk and the effectiveness of spreadsheet controls.

An alternative to training is to provide a central support team to walk the spreadsheet owner through the process. This has worked well for many organisations. It is not only more effective than classroom training, but it also helps the business achieve consistency in implementation of the spreadsheet risk management framework.

## **44. Is the intranet an effective tool for ensuring awareness of spreadsheet risk within the organisation?**

The intranet is an excellent tool for providing reference information for individuals. If possible, all spreadsheet risk management frameworks, processes and training should be made available on the intranet.

However, posting documents on the intranet is not a substitute for delivering training. Employees should be aware it exists, but their training should be delivered through discussions, lectures, practical exercises and online tests. A more interactive method is required to ensure the proper approach to spreadsheet risk management in the organisation is appreciated and understood.

## 45. What are the key spreadsheet risk management capabilities that should exist in any organisation?

All users of spreadsheets need to be provided with training to develop a basic level of knowledge. This should include:

- Awareness of key spreadsheet risks.
- Understanding of the minimum spreadsheet control standards.
- Understanding of the key indicators of a spreadsheet becoming critical.
- Knowledge of whom to engage when a spreadsheet is becoming critical.

Providing this level of training to all users can be challenging for many organisations. As a result, many businesses initially focus on those parts of the organisation that are more dependent on the use of spreadsheets.

In addition to this basic level of knowledge, the business will need access to people with much deeper skills who can provide support and guidance to the wider community. Some organisations have set up central teams with these deeper skills that the spreadsheet owners can draw on when required. Unless users are granted access to these types of people, it can be difficult to effectively roll out the spreadsheet risk management framework. The deeper skills required include:

- Risk assessment skills.
- Spreadsheet design skills.
- Advanced spreadsheet development skills (including Visual Basic development if macros are widely used in the business).
- Spreadsheet testing skills.

## 46. To what degree should the organisation expect to be sourcing third-party skills?

There is no requirement to make use of third parties. Many organisations have found it helpful, however, to draw on the experiences of other organisations when establishing a spreadsheet risk framework.

Skilled third-party resources have been engaged in a number of areas, including:

- Development of a spreadsheet policy.
- Identification and assessment of critical spreadsheets.
- Spreadsheet testing.
- Management assurance.

Organisations have gained value from employing experienced consulting firms to perform the initial identification of their critical spreadsheets. The consultants provide a level of independent evaluation but also draw on their experience with other organisations to accurately assess the inherent risk and complexity of spreadsheets. At the end of a project in which consultants have been employed, it is important for any organisation to ensure the processes have been embedded in their day-to-day operational processes.

Spreadsheet testing can be time-consuming, and experience has shown that it is unlikely to be effective when performed by the spreadsheet owners. There is a natural tendency for the spreadsheet owner to take shortcuts and perform a less thorough review. Third-party companies are able to leverage specialised testing tools that provide a higher level of assurance. Spreadsheet testing is, hopefully, a process performed through one-off projects, so there is an opportunity to agree to a relationship with a third party to ensure they are available to perform this work as and when required.

Management assurance exists to ensure that appropriate spreadsheet controls are in place and operating effectively. Organisations often do not have the luxury of internal risk teams with the capacity to perform extensive management assurance work. The alternative is to allow the spreadsheet owners to perform a self-assessment of the controls in operation. This is typically a good approach, but only when used in combination with some form of independent assurance work to ensure self-assessments are performed appropriately. Third-party firms can provide this capability on an annual or other scheduled basis.

Other services provided by third parties include:

- Evaluation of technology solutions in the marketplace.
- Implementation of a spreadsheet management technology solution.
- Assisting internal audit with spreadsheet reviews.
- Training and awareness on spreadsheet risk management.
- Development of appropriate control framework.

#### 47. Should the organisation be employing specific spreadsheet support teams?

To effectively implement spreadsheet risk management processes, the business will typically need to provide spreadsheet owners with access to people with deep expertise on an as-needed basis. The deeper skills required include:

- Spreadsheet risk management policy expertise.
- Risk assessment skills.
- Spreadsheet design skills.
- Advanced spreadsheet development skills (including Visual Basic development if macros are widely used in the business).
- Spreadsheet testing skills.

Some organisations have found that a cost-effective approach is to create a small pool of central resources that the business can draw on to provide deeper skills when required. This will depend, however, on the complexity of the spreadsheets used within the organisation. Organisations will not require specialised spreadsheet support analysts if the spreadsheet owners are capable of adequately controlling the spreadsheets they operate.

Some organisations employ spreadsheet support teams to ensure critical spreadsheets are developed in a controlled yet responsive manner to support business requirements. These teams essentially operate as a rapid development team, typically located alongside the operational staff they support.

The use of a spreadsheet support team needs to be carefully monitored to ensure all application development requirements do not go through the spreadsheet support team, as certain requests should go through the more formal IT development environment.

Successful spreadsheet support teams tend to operate in financial services organisations and typically in a trading environment where daily analysis and deal construction is performed through complex spreadsheets. (This is a good example of where more traditional applications are seldom flexible enough to support business requirements.) Some businesses also have used central support teams to provide training to the business on spreadsheet risk and drive the implementation of the spreadsheet risk management policy.

#### 48. Should formal processes exist to ensure that the organisation consistently manages spreadsheet risk?

A spreadsheet risk management operating model should contain documented processes and controls. Processes should exist to ensure that all individuals with spreadsheet risk management responsibilities can follow a consistent process.

Critically, controls also should be defined within these processes. These controls will have defined control owners responsible for their operation. Having documented controls ensures the organisation is able to evaluate the effectiveness of the spreadsheet risk management processes.

Spreadsheet risk management processes typically include:

- Policy definition.
- User training and awareness.
- Identification of critical spreadsheets.
- Individual risk assessment (assessment of risk in an individual spreadsheet).
- Overall risk assessment (consolidation and aggregation of risk information and associated reporting).
- Controls definition and implementation.
- Controls testing and assurance.
- Certification of spreadsheets (quarterly or annual certification by spreadsheet owners that they understand their responsibilities and that risk is being managed in accordance with policy).
- Compliance (process of gaining assurance that the business is in compliance with the spreadsheet risk management policy).

# Technology enabling effective spreadsheet risk management

## 49. Do technology solutions exist to help with spreadsheet risk management?

There is a relatively new market for technical solutions to assist with spreadsheet risk management. Many of the more established vendors have been operating in this area for only a few years.

Ventana Research has conducted research within this area and estimates that while the total market for enterprise spreadsheet management tools was \$15 million in 2006, this will grow to an estimated \$500 million by 2011. In our view, this estimate is conservative given the reliance placed on spreadsheets by so many companies and the increasing scrutiny and compliance requirements being placed upon them.

The types of technical solutions available can generally be categorised into three groups:

1. **Spreadsheet management/control:** These solutions typically provide change control, version management, change history (audit trail) and security over those spreadsheets managed by the solution. Some solutions can be used to restrict access to functionality or specific cell ranges.
2. **Spreadsheet search/discovery:** These solutions perform automated scans of networks or specific servers to generate an inventory of all spreadsheets discovered. Some solutions perform limited analysis to help the user deal with the large number of results typically generated.
3. **Spreadsheet auditing:** These automated tools assist a reviewer when auditing a spreadsheet. Although some element of manual review is still required, these tools, when used correctly, greatly improve the efficiency of such reviews.

## 50. Are there established solutions and clear market leaders?

The vendors are a mixture of new companies who are specialising in this particular market and several existing software vendors who have diversified their existing product range.

Although some solutions are more established than others, the market is still relatively immature and gaining new entrants. No clear market leader has yet emerged, partly because the right choice of solution (or combination of solutions) will depend on individual companies' requirements and goals.

Given the rapidly changing state of the market, it is difficult to provide detailed information in a publication such as this. Protiviti does, however, maintain information on all of the leading solutions and would be pleased to provide further information on request. Though there is clearly a large market, we believe the current number of vendors is unsustainable, and that some consolidation will occur.

## 51. If technology solutions are implemented, will they impact all spreadsheets operating within the organisation?

The spreadsheet management and control solutions are typically used only to manage spreadsheets that have been identified as business-critical or 'in scope'.

It is theoretically possible to monitor and manage all of the organisation's spreadsheets, but it would normally be impractical given the number of spreadsheets that exist in most organisations. We recommend, as part of the solution implementation, that careful consideration be given to determining which spreadsheets should be included. The rules for determining which spreadsheets are in scope should be defined in the spreadsheet risk management policy.

## 52. Are there performance or usability issues that need to be considered when implementing spreadsheet control solutions?

This depends on the individual solution and how it operates. Some solutions place limitations on user functionality. Others may increase the time it takes to save large spreadsheets or may generate significant volumes of data traffic on the network. Companies should ensure that they evaluate any usability and technical constraints and requirements during the product selection process.

## 53. Who would implement and manage the operation of any spreadsheet solutions?

Typically, the implementation of such solutions is run as a project, with a dedicated project team reporting to both business and IT stakeholders. The business will want to ensure that the solution and its associated processes meet their objectives. IT often will require the solution to fit with their technical architecture and not adversely affect network performance. IT is also likely to have responsibility for maintaining the platform going forward, and therefore, will need to be involved in the selection and implementation processes.

Often, the solution also will require a system administrator role for technical assistance with matters such as setting up new users. Additionally, there is likely to be a requirement for a business manager or reviewer to ensure that changes made are appropriate. The actual roles will depend on the objectives and the solution(s) chosen.

**54. Is it as straightforward as installing the software in order to manage the risk or to be compliant?**

Unfortunately, spreadsheet risk management is not as straightforward as simply implementing a tool. In fact, the selection and implementation of a spreadsheet risk management tool is potentially one of the easiest parts of the overall programme.

Before implementing a tool, the business will need to determine its risk appetite and policies governing the use of spreadsheets. Then, the business will need to educate all users of potentially critical spreadsheets and embed a risk management culture. This is typically the most complex part of any spreadsheet risk management programme.

Once the business has identified the potentially critical spreadsheets that will be controlled using the selected tool, the spreadsheet owner will need to perform testing to ensure the spreadsheet is operating effectively. (There is limited value in tracking changes to a spreadsheet that lacks integrity from the start.)

The spreadsheet owner then will need to decide what actions/ changes should be logged and review responsibilities. There is no point in building up an audit trail of all the changes made to a spreadsheet if nobody reviews and follows up on the changes. The spreadsheet owner also must consider access control requirements, and the spreadsheet risk management tool will need to be configured appropriately to manage this access.

# About Protiviti Inc.

Protiviti ([www.protiviti.co.uk](http://www.protiviti.co.uk)) is a global consulting and internal audit firm composed of experts specialising in risk and advisory services. The firm helps clients solve problems in finance, operations, technology, litigation and GRC. Protiviti's highly trained, results-oriented professionals serve clients in the Americas, Asia-Pacific, Europe and the Middle East and provide a unique perspective on a wide range of critical business issues.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

## End-user computing risk management services

Protiviti has the experience to help you understand the risks associated with your end-user computing applications. We can help you implement an effective spreadsheet risk management framework that provides an appropriate level of control without adversely impacting usability or productivity. Our approach represents a pragmatic response to end-user computing risk based on real business need and built on practical experience.

Protiviti knows what auditors are looking for in respect to statutory and compliance requirements, and can help you interpret and meet those requirements. We remain vendor-independent but have thorough knowledge of the solutions on the market. With this knowledge, we can help you:

- Define spreadsheet risk management policies and supporting processes.
- Evaluate the options available based on your specific requirements and objectives.
- Create an inventory of spreadsheets through scanning or targeted discussions with users.
- Review spreadsheets to identify errors and develop a base-lined version that can be controlled.
- Implement a spreadsheet management framework, including:
  - Select a spreadsheet risk management tool.
  - Determine what controls and settings should be configured within the solution.
  - Develop procedures, training/awareness programmes and monitoring processes.

We also help internal audit functions add value through auditing end-user computing, including:

- Assessment (pilot study or full assessment) of the extent to which end-user applications support critical business processes and the risk these applications present to the business.
- Identification and assessment of controls in place around the development, operation and maintenance of end-user applications.
- Audits of individual applications to identify potential errors and design weaknesses, using automated tools and our spreadsheet audit methodology.
- Remediation of identified control gaps and applications errors.

# Contacts

## **EMEA (Europe, Middle East and Africa)**

**Jonathan Wyatt**

**Managing Director**

+44 (0)20 7024 7522

jonathan.wyatt@protiviti.co.uk

**Ewen Ferguson**

+44 (0)20 7024 7531

ewen.ferguson@protiviti.co.uk

**Rob Nieves**

+44 (0)20 7389 0445

rob.nieves@protiviti.co.uk

## **United States**

**Edward Hill**

**Managing Director**

+1 713 314 5010

edward.hill@protiviti.com

**Evan Campbell**

+1 713 314 4974

evan.campbell@protiviti.com

**Andrew Struthers-Kennedy**

+1 410 454 6879

andrew.struthers-kennedy@protiviti.com

## **Asia-Pacific**

### **Singapore**

**Matthew Field**

**Managing Director**

+65 6220 6066

matthew.field@protiviti.com

**Raymond Ang**

+65 6220 6066

raymond.ang@protiviti.com

### **Australia**

**Justin Trentini**

+61 2 8220 9502

justin.trentini@protiviti.com.au



Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

Protiviti is an Equal Opportunity Employer.