

**VANSON BOURNE**

## **The Risk of Sharing**

**January 2005**

## Foreword by Workshare

'Integrity' is a word that is conspicuously absent from many areas of business process. Efficiency is more commonly used as the mantra that defines operational success. Efficiency is something that executive teams battle with on a daily, quarterly, and annual basis. Inefficiency hurts the bottom line and there is a constant search to eradicate its presence from all areas of business. Efficiency equates to speed, streamlining and automation, all common points of reference when considering the role of technology in business today.

There has been no greater contributor to efficiency than the development of the internet. However, with its development, an additional priority has been forced into the efficiency equation; that of security. As the world got 'connected' it also got 'infected' and companies soon began to realise that to do business across the internet did not come without risk. Viruses could bring down the network and hackers could dial into corporate assets.

As the internet came of age, another trend was forcing industry to reconsider its operational processes and procedures. Organisations, such as Enron and Parmalat brought corporate accountability to the top of the boardroom agenda with dramatic effect. Regulatory compliance is an issue that has stoked corporate fires following the arrival of heavyweight legislation, such as Sarbanes Oxley, to bring business under much closer scrutiny. With both security and compliance, document processes are brought into question.

In the context of security and compliance, efficiency is given a new dimension. Speed and automation are no longer enough. Today, organisations have to be more accurate and accountable. The efficiency of a process is synonymous with the integrity of a process. Efficiency without integrity increases risk and liability, yet many businesses operate today without sufficient consideration of both. However, that situation is changing. Juniper Research estimates that market for corporate document security applications will grow to \$274 million by 2008, primarily driven by factors such as compliance and legal requirements.

How does the document production process change with greater need for integrity? If measures are implemented without sufficient thought as to the security, accuracy and compliance of the process, they are inherently inefficient and ineffective. The new mal-ware is one that is hardly recognizable. It is the inadvertent release of information found in seemingly benign documents. Most businesses don't have a strategy to combat it. Therefore, integrity must be part of any document strategy and has a direct impact on performance.

The *Risk of Sharing* Report 2005 explores the integrity and efficiency of a process that is pervasive across most areas of business: the creation, amendment, approval and distribution of documents. Any organisation that creates information, captures it in a document and shares that information with others, should find the report of value. In an area that we have defined as 'Document Integrity', there are several insights into how the way we create and share information presents an evolving set of challenges for businesses looking to lock down and secure their ever more transparent document processes.

*Joe Fantuzzi, CEO and Chairman, Workshare*

## The Risk of Sharing – Executive Summary

The *Risk of Sharing* report investigates the scale, awareness levels and efficiency of processes that impact document integrity. From assessing how risks, such as security and compliance, are exposed in the document process, to establishing productivity gains and losses, to putting document integrity in context of other business administration tasks, the report finds that:

### Security & Compliance

- Document security is a priority for the majority of organisations taking part in the study. On average, 51% of respondents agree that document security is a priority
- An average of 35% of documents contain legally sensitive information. This number increases to over 50% with a third of businesses taking part in the study
- One in four of all documents in circulation is subject to regulatory compliance
- There is an exceptionally low awareness regarding the level of risk associated with document amendments and approval - 90% of business users are not familiar with the term metadata
- Business users consider themselves personally accountable for document security

### Accuracy & Efficiency

- Amending and approving documents via email is considered a greater barrier to efficiency than spam. 59% of respondents consider document attachments to be the biggest burden on their email working day
- On average, business users spend 2.5 hours per day approving and amending document attachments
- There is a lack of faith in the existing technology available to manage document content. 78% of respondents refer to hard copy documents, rather than on screen documents, when managing complicated approval processes
- There are significant levels of process surrounding documents but many are inefficient and compromise document integrity

From the new report findings, which build a picture of document integrity and the associated risks, the following conclusions are made:

- There is a high level of exposure to security and compliance risk created through poor document integrity processes
- Accuracy of information can be compromised with poor document integrity processes
- Many existing document technologies do little to negate the risk of compromising document integrity
- The resource burden related to the amendment and approval of documents should be given greater priority
- Lack of understanding in how document integrity can be compromised requires companies to evaluate how they tackle the problem
- Assessments should be made on how efficiencies based on document amendment, approval and distribution can be improved

Though internet-based threats to document integrity are well understood and placed high on the IT agenda, businesses are creating a new set of risks that impact security, increase compliance risk and compromise end user efficiency. As these risks to document integrity come mostly from the inside, created without malicious intent, most businesses are not geared to recognise, or respond to them.

The *Risk of Sharing* report was conducted across three international regions, the United States, the United Kingdom and Australia, petitioning representatives from 100 organisations in each area. Vanson Bourne, a leading B2B market research consultancy, conducted the survey in November 2004. Respondents for the survey are defined as business users responsible for the amendment and approval of company documents.

## The Risk of Sharing – Section One – Inside Out Security Risk

Document security is most commonly referred to in terms of hacking and secure storage of information. What many companies are unaware of is the level of security risk that resides in the content of the document itself. Arguably, we have a one-dimensional view of security in document terms, looking at access and passwords, placing information under a digital lock and key. With the increasingly complicated nature of information security, there is a need to add breadth and depth to this understanding.

In Figures 1&2 we see that there is a high level of information residing in documents that could increase the security risk, or increase the need for greater focus on the compliance and accuracy of the documents we share.

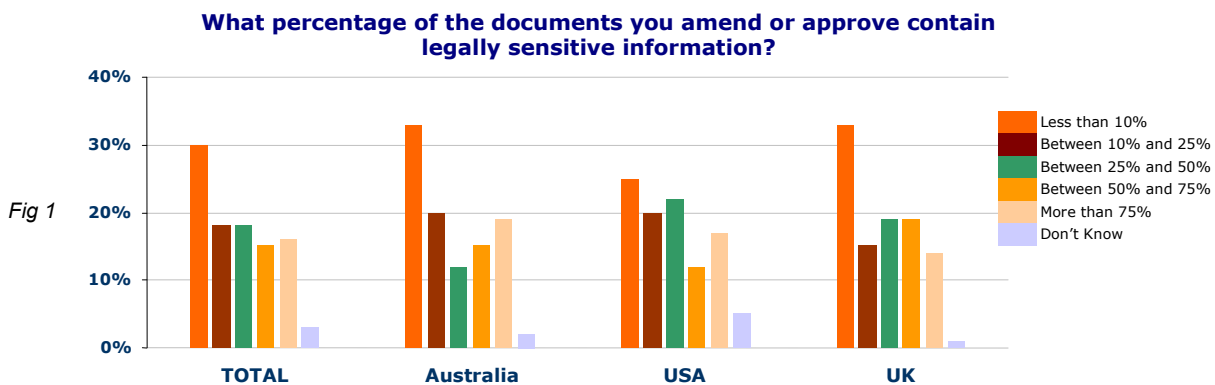


Figure 1 shows the range of legally sensitive information that exists within business documents across the three international regions. From the varying degrees of sensitive documents, the mean average is 34%. Therefore, one in three documents circulating between an organisation and its third parties contains legally sensitive information. In other words, information that requires an increased level of content security. Typical documents in this category may include contracts, proposals, bids, service agreements and confidential reports. It is also the case that on average, 31% of businesses consider at least half, and in many cases over 75%, of the documents that are amended, approved and circulated each day contain legally sensitive information. These are businesses in a 'high document risk' category.

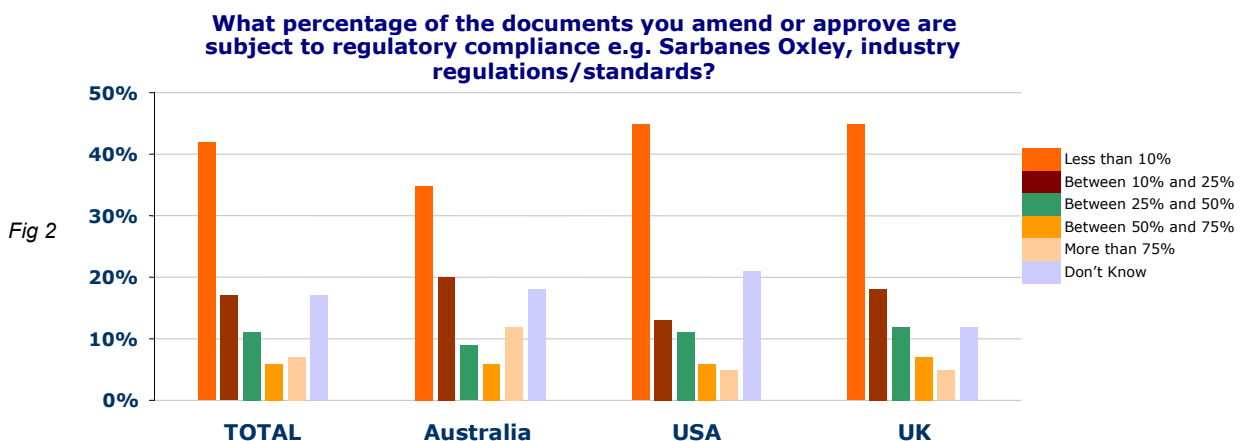


Figure 2 (previous page) asks a similar question to Figure 1, only this time regarding the percentage of documents that are subject to regulatory compliance. The average number of documents in this instance is slightly lower with one in four (23%) of documents having a compliance obligation. Within the area of compliance, there is a much higher percentage responding to 'Don't Know', which, given the complexity and level of ambiguity in the area of regulatory control, is not surprising. It is also worth considering that, when looking at compliance, especially legislation such as Sarbanes Oxley, potentially *all* or *any* of the business documents created or passing through an organisation are subject to regulatory control. Arguably, the business user perception of compliance and its relevance to documents they create and exchange does not necessarily reflect the overall corporate picture.

**Document security is a priority in my organisation**

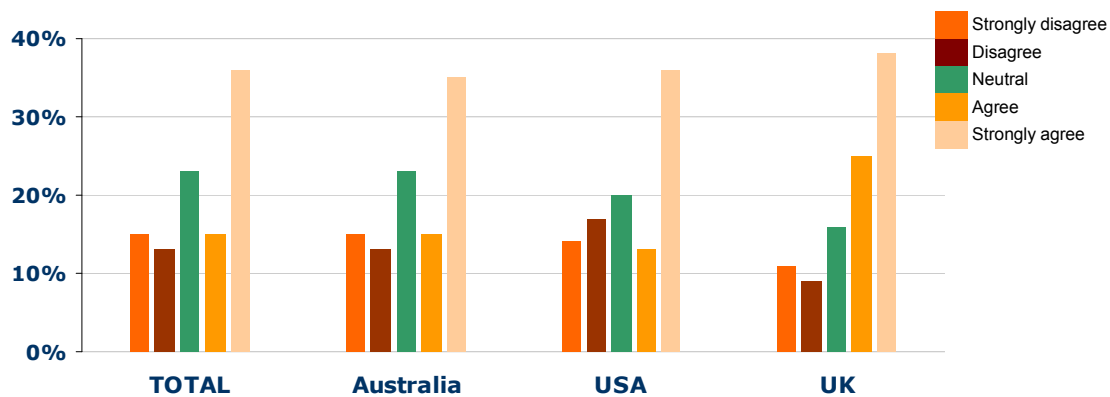


Fig 3

Figure 3 shows that there is a significant priority given to the security of documents by half the respondents in the survey. 51%, on average, of business users agree, or strongly agree that document security is firmly on the business agenda. In conjunction with the high level of legally sensitive information in circulation across the organisation, it is encouraging that half of the companies surveyed have considered the importance of locking down document content. A healthy majority (72%) of those who consider document security as a high priority are those identified in a 'high document risk' category from Figure 1.

From these first three graphs, we begin to build a picture of where security sits in relation to overall document integrity. There are a lot of documents 'in the wilds' of amendment, approval and distribution that contain sensitive information, building the need for document integrity. There is also the need for adherence to regulatory control and approval in many cases, another area where integrity may be scrutinised.

When assessing the significance that document integrity should have in your organisation, it is important to establish how many documents are in circulation at any one time, as this is a way of quantifying the potential risk to the business. One in three, or one in four documents may seem at first glance a low percentage but, in global terms, it refers to billions of files that are being continually altered and sent from one party to another during the course of the business day.

One of the main problems with content security and the integrity of documents is the need for tighter control around the area of metadata. This is information that resides in document files and holds the 'DNA' of a document's history. Figure 4 shows immediately that there is a low level of awareness around this issue for business users. Most respondents (80%) have no understanding of the term. Of the 20% that do understand the term, only half could accurately define it.

**Are you familiar with the term metadata?**

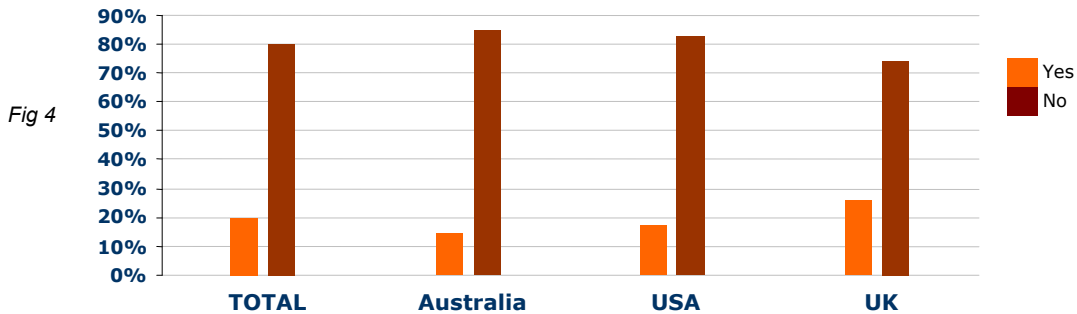


Fig 4

Though startling at first glance, metadata is a technology term and would not necessarily enter the business vocabulary. But it does demonstrate that, with such a low level of awareness in this area, the potential risk of inadvertent disclosure of information through documents containing rogue information (hidden in document metadata) is potentially very high.

A lack of awareness also suggests a lack of control, meaning business users leave their fingerprints all over documents, showing information not intended for end user consumption. Another key finding from the survey is that 70% of respondents do not create documents from new, and will either copy existing documents, or use corporate templates – both of which run the risk of old information finding its way into new files.

So, who is responsible for ensuring that document security is maintained? Figure 5 suggests that the majority of respondents (50%) feel there is a shared responsibility for document security. Of those who feel responsibility should sit with an individual, there is a split between the author of the document and the IT Department on 'carrying the can'. The mix of responses highlights a lack of process in the area overall.

**When you are altering or amending documents, who do you think is responsible for ensuring that the document data is kept secure and not inadvertently disclosed?**

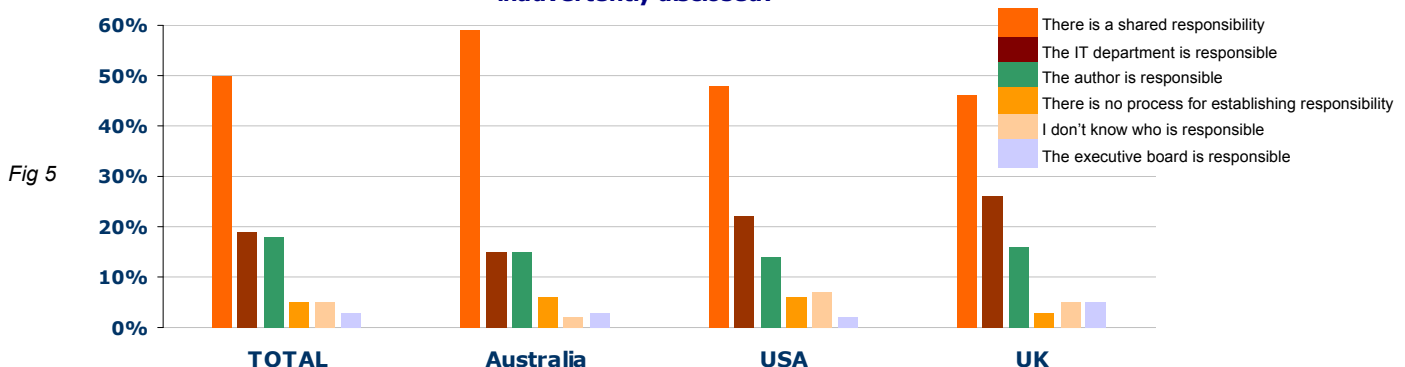


Fig 5

Shared responsibility seems logical and fair, but could lead to confusion. IT definitely has a role to play in document security, but volume of documents alone makes it very difficult for an IT department to be wholly responsible, particularly when we look at security in context of document integrity. The author of a document should be a strong contender for security ownership, but most documents are rarely the work of one person so the lines of responsibility blur, regardless of who is selected as a *document security officer*. Therefore, it has to be the process itself, rather than the individual that ensures document integrity is maintained.

## The Last Amendment

Though the end user may be forgiven for not knowing the term metadata, it appears that there is a high level of personal responsibility for document content. Figure 6 shows that on average 57% of business users feel personally accountable for their input into a business document, with 19% believing there is a shared responsibility for amendments made to documents and 15% 'passing the buck' to management.

**When you are altering or amending documents, who do you think is accountable for the content**

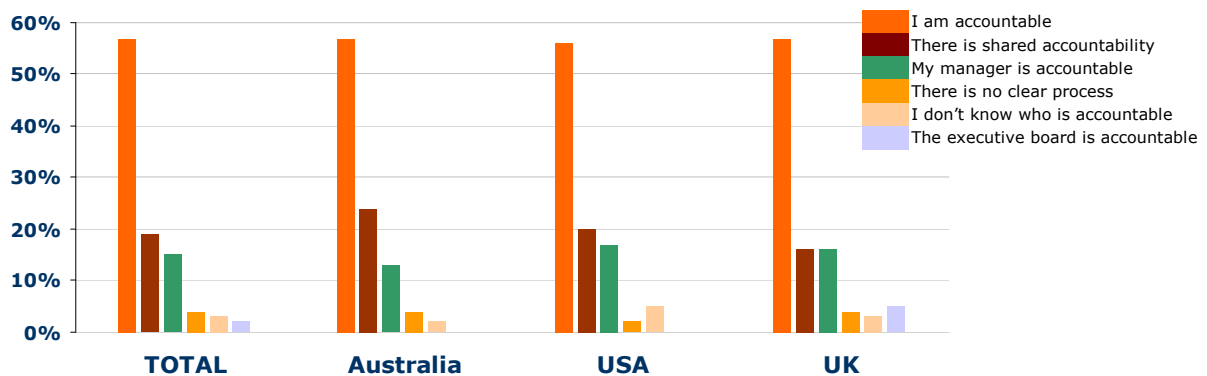


Fig 6

As with the previous section, the issue of accountability presents an interesting question. Clearly, in most cases, the individual feels accountable for their actions. However, by definition of the output itself, individual responsibility for contributions does not address the issue of accountability of the entire process. An average of five people will input into a business document, but in some cases, especially in the Legal and Corporate Finance sectors this can be anything up to 20 contributors per document. Who takes responsibility for the content? The answer will vary between organisations but high levels of individual accountability points towards a low level of development in the overall document process.

## Section One - Summary

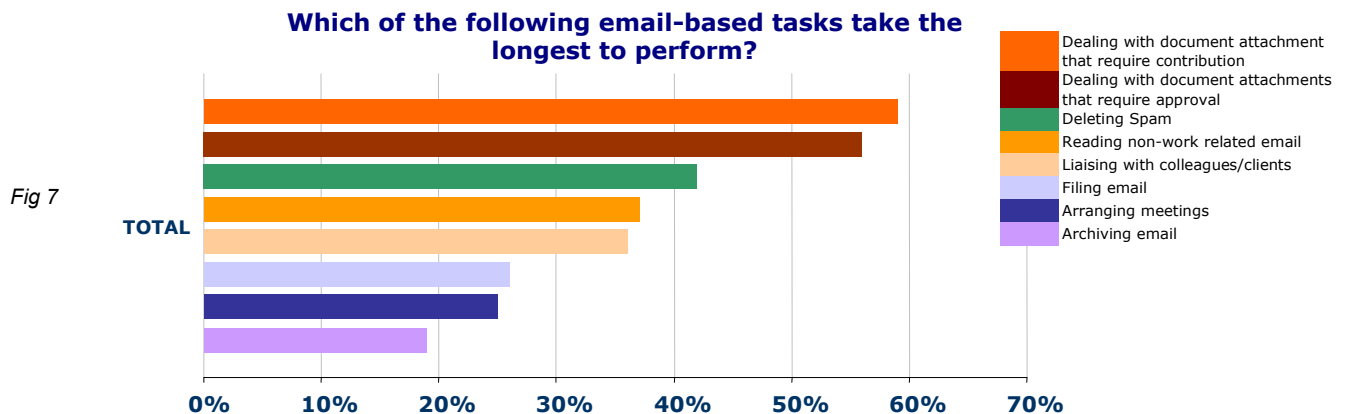
- Document security is a priority in half of the organisations surveyed
- On average, one in three documents contain legally sensitive information
- 31% of respondents work in a high document risk category
- On average, one in four documents are subject to regulatory compliance
- Business users have low awareness of how document integrity can be compromised by metadata exposure
- Ownership of document changes and document security varies significantly, creating accountability gaps

## Section Two – A Burden Shared...

Security and compliance are key components of a document integrity strategy, but there are additional considerations in the management of sharing information that are discussed in this section of the report.

Accuracy and efficiency form a large part of a document integrity strategy. Though risk in the context of accuracy does not come in terms of regulatory control, or inadvertent disclosure of information, erroneous documents can compromise corporate success and impact end user efficiency directly.

To galvanise this point, let us first look at the responses set out in Figure 7, where we assess the level of resource burden created by the ‘actioning’ of email attachments in relation to other common email tasks. Evidently, the amendment and approval of email attachments is a heavyweight part of the working day. Most attachments come with a resource-sapping payload that puts them ahead of Spam and Administration in the ‘inbox burden’ league. In among the corporate concerns surrounding Spam today, it appears that there are equally frustrating aspects to managing the influx of document attachments that arrive in our inboxes on a daily basis.



To understand the resource burden in this area, the *Risk of Sharing* report asked respondents to quantify the amount of time taken to deal with the amendment and approval of email attachments each day and the number of document attachments dealt with.

Responses showed an average of 6-10 document attachments requiring significant attention each day (per user) and an average of 25 minutes taken to deal with each document. This equates to an average of between 2 to 2.5 hours per day dedicated to business users amending and approving document attachments.

Clearly, there is a distinction between inbox Spam (a nuisance, sent without request) and documents attachments (a critical aspect of business practice). But it is interesting to look at document attachments in the context of Spam and other inbox tasks. What Figure 7 provides us with is a snapshot of a business user’s inbox and the resource dedicated to the various tasks that make up the inbox working week. The important point to understand is that the creation, amendment and approval of documents via email is a significant aspect of business users’ working lives, which means it has to be responsible for a large part of their personal productivity.

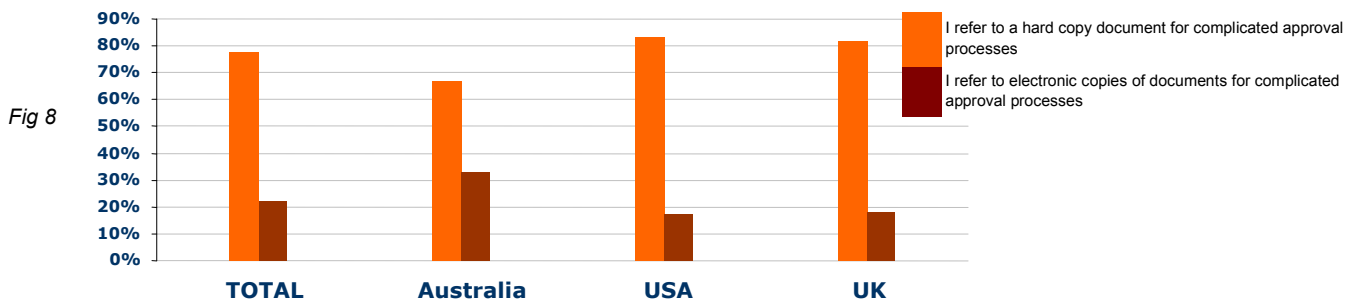
## Faith in Technology

As a business process, document integrity is defined by the technology that surrounds it. In broad terms, the two IT elements are the document formats that create the files and the emails that carry the information. From a compliance perspective, there is also a demand for technology to manage author and amendment audit trails. For collaboration, portals and new sharing environments, such as Microsoft SharePoint, are also used. From the respondents taking part in the *Risk of Sharing* survey, the table below shows the percentage use of common tools at our disposal.

Spell and grammar check	85%
PDF	67%
Document compression (e.g. Winzip)	51%
Track Changes	28%
Collaborative intranet/portal	16%

Though there are a number of tools at the disposal of business users, Figure 8 shows that the majority express a lack of faith in the technology available to deal with detailed, or complicated approval and amendment processes. An average of 78% of respondents refer to hard copy documents where detailed documents are involved. No doubt, there is a simple human preference in trusting 'pen and paper' beyond 'files and data', but Figure 8 also points towards that fact that most desktop tools at our disposal lack the necessary functionality needed for business users to embrace them.

**Which process do you prefer to use for detailed/complicated approval and amendment?**

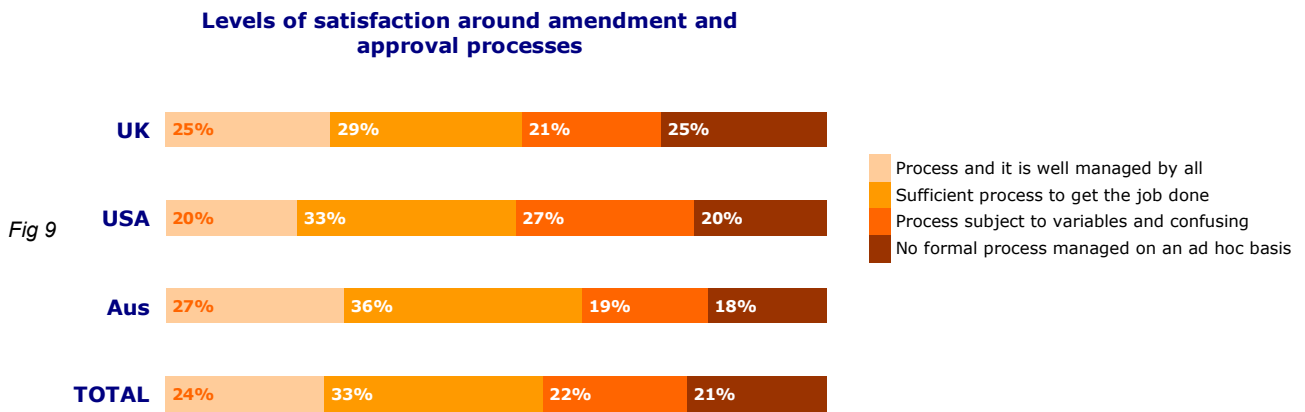


Looking ahead, it seems obvious that this picture has to change. The pen and paper approach to maintaining document integrity compounds the complexity of the process and interrupts effective workflow. More importantly, when assessing risk from the perspective of accountability or auditing, it creates gaps in the document trail.

## Levels of Process

Currently, there is little standardisation in the processes surrounding document integrity. All we can assume is that most businesses create and share large amounts of documents internally, or with third parties, and that most documents are the work of multiple authors. How organisations manage this process will vary, as shown in The Risk of Sharing report already from the levels of security, legal sensitivity and compliance required of business documents by different respondents.

Despite the variables, there are some areas of common ground shared by the significant majority. The majority of businesses (95% of those surveyed for the *Risk of Sharing* report) use Microsoft Word to create documents, and the most common mechanism for sharing information is email, or an intranet/portal. Figure 9 assesses the levels of satisfaction business users have with existing process around document amendment and approval. The responses can be grouped into two areas, those happy, or at least satisfied with existing processes, and those confused by the process, or those that have no formal process at all.



The graph shows that opinion is largely divided on the issue of process satisfaction, but that there is approximately a 55% to 45% split regarding levels of satisfaction. However, only one in four (one in five in the case of the US) consider existing processes to be watertight. Taking this into account, there is clear room for improvement with the majority of respondents to develop greater efficiency and/or satisfaction in the processes.

By the nature of the variables involved, figure 9 can only serve as an indication of efficiency. However, when applying these responses to other areas of the document integrity equation, it exposes areas of concern. How secure is process if it is subject to variables and confusing? Is something with no formal process, conducted on an ad hoc basis generating unnecessary compliance risk? What level of accuracy or quality is there in the output of a process that is merely sufficient? As with any new area of business, the satisfaction in the status quo often belies vulnerabilities or efficiency gaps when set in context of the evolving nature of the business process behind it.

## Section Two - Summary

- Amending and approving document attachments drains business user resources
- Business users in the survey spend an average of 2-2.5 hours managing email document attachments
- 78% of respondents prefer working on hard copy documents for complicated approval processes
- Hard copy amendment and approval increases the risk of gaps in the document audit trail
- On average, only one in four businesses has a robust approach to the processes surrounding document integrity

## The Risk of Sharing – Report Summary

Businesses that acknowledge the need to address document integrity must first establish how existing processes measure up to scrutiny. An assessment of the questions posed in the *Risk of Sharing* report provide a good starting point:

- How many documents does your organisation circulate containing legally sensitive information?
- How robust is the security around the amendment and approval processes?
- Could poor document processes compromise regulatory compliance requirements?
- Are business users in your organisation aware of metadata risk?
- Are there clear areas of ownership in your organisation for document content and security?
- How much time is wasted on *ad hoc* processes surrounding document amendment and approval?
- What are the existing levels of satisfaction around document integrity processes across the organisation?

Surveying business users provides an insight into document integrity that IT departments may not have previously been aware of. The business user perspective provides picture a broader of where risk resides in the world of document content, which allows for a more informed decision as to the right tools and processes to bring document integrity under control.

An insight into the nature of document content is critical to any organisation that places high value on the information it creates and shares. The *Risk of Sharing* report shows that many organisations could do more to ensure robust levels of precision and control, in order to improve document integrity.

Many of the findings in the survey point towards the need for tighter control in document processes. Awareness of the risks involved in sharing information is a significant first step in achieving this. Increasingly, there is the need to maintain and manage a complete document lifecycle history in order to be transparent and accountable to internal and external audiences. Whilst many organisations begin to address this from a workflow perspective, most still look at documents in terms of files, rather than concerning themselves with the content itself.

During 2005, many organisations will take measures to ensure that processes surrounding document integrity are robust, which will minimise risk in a number of areas where business users are creating and sharing information. To help in this process, the *Risk of Sharing* report has provided a top five recommendations for any individual, or team, tasked with creating an integrity strategy.

Document integrity may be a new concept to many organisations reviewing this report, but the need for tighter control on document security, compliance and accuracy should be a logical step for them to take. In its objective to investigate the scale, awareness levels and efficiency of processes that impact document integrity, the *Risk of Sharing* report should prove valuable to any organisation that believes documents are an integral part of the business environment.

## Top Five Recommendations

### Review Internal Controls

An understanding of existing controls and processes is the starting point for establishing an integrity strategy for document content. From the report, we see that levels of control will vary across different organisations. Some businesses may only need to fine tune existing practices, others may have no policy or controls in place. A straightforward analysis of how content is created, who has responsibility/ownership of the content and what tools are used to automate, or assist in the process provides a framework to get an internal review underway.

### Monitor Worker/Business Processes

Before making wholesale changes to any process, it is important to monitor how it is used throughout the business. There is no such thing as a single document process, the document type and the various stakeholders involved are too varied to have a 'one size fits all' approach to the document integrity issue – hence the need to always factor *ad hoc* working into any departmental, or company-wide process.

### Analyse Areas for Improvement

Reviewing and monitoring areas of control and process allows for analysis of areas of improvement. On revision, it may transpire that workflow and review processes in most cases are robust, but potential security and compliance risks are being ignored, creating a need for improvement in this area. Outside of the processes themselves, it may be that certain parts of a business have established high levels of document integrity, but other workgroups and departments are lagging behind. Analysis of these areas will identify the document integrity 'hot spots' across your organisation.

### Pilot Improvements in Target Groups

Having invested the time and energy in establishing criteria for a document integrity strategy, piloting processes in key document groups is an important next step. It's not just a question of ironing out the creases of implementation and adoption, live testing may provide further insights into addition process/user benefits of a new workflow and procedures. At this stage, it is important to understand that structured systems to monitor and manage document content will not always solve document integrity problems. Workflow is best served by 'always on', fluid monitoring that supports *ad hoc* workflow.

### Allow for Evolution

Once completed, documents tend to be static, but the processes are always subject to change. Regulatory control, organisation changes and developments in how companies use technology to create and share documents will demand that the document strategy evolves with them. Also consider that the document integrity strategy will facilitate an evolution in itself. Maintaining logs of document activity, tagging document audit trails and achieving greater visibility of document paths and lifecycles will enable greater flexibility, accountability and efficiency in future.

For further information on The Risk of Sharing please contact Workshare on:

UK: +44 (0) 20 7426 0000

US: + 415 975 3855

HK: + 852 2251 8985

e-mail: [riskofsharing@workshare.com](mailto:riskofsharing@workshare.com)