



2. Business Advisor Series

Don't Risk your Business

How to ensure your software is licensed

What Risks is your business running?

In 2007 the Business Software Alliance (BSA) asked independent research house GfK NOP to investigate the attitudes of Small and Medium Size Enterprises SMEs across Europe towards software and their awareness of the associated risks of using unlicensed software (including counterfeit copies). The results revealed 95% of SMEs claim to be 'confident' that all of the software installed is fully licensed. However, in-depth analysis by IDC shows that software piracy across Europe remains high, with rates in Western Europe running at 34% and in Central and Eastern Europe at 68%.

This discrepancy between the perceived situation and the reality suggests a lack of awareness among business executives with regards to software and its management. This is a dangerous situation. Software has fast become one of the most valuable and critical business assets a company has. If businesses are not investing in, and appropriately managing and protecting their software assets, they leave themselves open to numerous business risks that can have significant financial implications.

The Business Software Alliance has produced this guide to outline the real risks of unlicensed (pirate, mis-licensed or under-licensed) software, how you can protect your business, and how you can maximise the benefits of the software you use.

Definitions:

Unlicensed software: any software product that has been installed onto a PC when the license agreement does not allow or support that installation or no license/ usage agreement has been made with the copyright owner. In this document the term 'unlicensed software' is used to refer to all three forms of software copyright infringement listed below.

Under-licensed software: software that has been over-installed onto more PCs than the licence agreement allows. For example a licence may support the software being installed onto 20 PCs. If the software has been installed onto 30 PCs, the additional ten installations are considered 'unlicensed'.

Mis-licensed software: software that is being used for purposes not permitted under the licence agreement. For example, software licensed for academic use that is used for commercial purposes.

Pirate software: any software that has been deliberately copied (on a significant scale) to defraud the copyright owners through illegal distribution, either using CDs or via Internet download sites. This includes 'counterfeit software'.

Foreword

For many SMEs, the world of risk management is changing rapidly with greater emphasis on governance and transparency and a seemingly relentless push towards tighter regulation. Many feel battered by the constant stream of messages encouraging them to become better at managing risks. But what are the business benefits? Why should attention be paid to aspects of risk management such as Software Asset Management and Information Security?

SMEs represent the vast majority of companies worldwide. In Europe they account for well over half of the wealth generated annually and employ the vast majority of most countries' workforces. Resistance to acknowledging or preparing for a major interruption to business leaves many firms potentially vulnerable to even a small interruption – putting at risk, collectively, tens of thousands of jobs and threatening the numerous other companies they interact with as suppliers or customers.

Managers in SMEs are used to dealing with the business challenges of changing supply prices, new competitors and demanding customers. Familiarity with such day-to-day challenges may breed over-confidence in the firm's ability to cope with disaster – even on a small scale.

The total impact of a business interruption incident may also be underestimated. A study by Gartner Consultants, suggests that 40% of businesses fail within five years of surviving a major interruption to business operations. In a separate study, they suggest that businesses that take more than 30 days to recover normal business operations are 'highly likely' to go out of business.

Given the heightened awareness of vulnerability today, it is perhaps surprising that so many businesses are unprepared for business interruption. This fact is widely recognised, but the reasons why are rarely discussed.

Our research at Henley shows that a significant factor in companies choosing to invest in risk management activities is the perceived weight of sources of threats set against the firm's risk appetite. However, as all SME senior managers know well, profits are the rewards for successful commercial risk taking. As an essential component of profit, business risk is unavoidable.

Managing risk is not simply about risk-reduction. It's about understanding the firm's appetite for risks and mitigating these by reducing their probability and/or impact as far as possible without inhibiting the firm's business. With optimally managed risks, the firm can safely tolerate increased exposure, increasing potential profits without exceeding its risk appetite. Good risk management increases the firm's resilience.

Many firms fail to recognise the role risk plays in their business operations. Larger firms have a structured approach to new project investment, factoring risk into return expectations. However, smaller firms may not always apply such rigid methods, potentially leaving them over-exposed as they grow.

Whether this is a result of a managing director's focus on cash-flow or drive for scale, smaller firms may be risking the livelihood of the entire business by growing without considering management of risk.

This is having an impact on Information Security risk management and the picture will be complicated further in the near future with the emergence of new technologies. The development and implementation of new types of computing and software distribution mechanisms will have a significant impact on the requirements demanded of risk assessment approaches.

Last but not least, we should not forget that it is those risks that are perceived directly that are dealt with using judgement (risks such as crossing the road for example). Unfortunately too many risks associated with software are still perceived as 'virtual'. Whilst most managers in SMEs will have experienced a faulty hard drive or a computer virus, few will have had to deal with very serious consequences. Although few major disasters can be linked to software, they have happened in large and small organisations alike.

The legal implications of operating unlicensed software can be significant, but what is perhaps less publicised is that operating licensed software means access to technical support, enhanced protection against viruses or malware, and therefore fewer interruptions. In a world where business continuity is key, SMEs are less able to weather the storm of business interruptions than larger firms. They typically don't have the same resilience inherent to large organisations which possess multiple premises, cash reserves, and sources of outside advice. As the research and advice presented in this report shows, it is often in fast growing small firms that not enough attention is paid to important risk management activities such as software licensing audits. Yet they are the most vulnerable.

As this guide indicates, recognition of this increased vulnerability appears to be low, indicated by the reported lack of activity and preparation. What then can we do about it? And what should we do? I suggest that we need to be more open about the consequences of poor risk management, and the benefits of good risk management.

Too often we hide problems because we fear that there will be a negative impact on our reputation. Yet it is only by communicating with our peers that we can develop effective risk management strategies that place the right management attention on those few risk management activities

that really matter, and ensure that we can carry on reaping the rewards of successful commercial risk taking, and avoiding the pitfalls of misguided risk taking.

This guide contributes to this communication effort. As far as software licensing is concerned the risk-reward equation is actually very simple. The operational and 'reputational' benefits of full software licensing are high. The rewards of inadequate licensing are not only low – they are unmanageable and at the root of even greater risk.

Jean-Noel Ezingard,
Henley Management School.



Software and Business Risk

Software is one of the most valuable assets a business has; recent research from the Business Software Alliance revealed that 94% of businesses across Europe cite IT as being essential to the successful operation of their company¹. Specialist software enables firms such as architects, engineers, scientists, financial organisations, and designers to compete and innovate. But even in day to day business practices almost every company relies on spreadsheets for managing financial activities, databases to hold vital information, email to communicate (with colleagues, customers and suppliers), and desktop publishing packages to create presentations and marketing collateral.

So it may come as a surprise to hear that 36% of software in businesses in the European Union is used without a valid licence².

Ignorance of the status of software licences within a company offers no defence, so it is vital that organisations are fully aware of both the risks of software piracy to their business, and the steps they can take to avoid those risks and ensure that they are acting legitimately.

Just as a business has to manage its employees appropriately and within certain legislative requirements, the same is true of the software that it uses. While most businesses are aware of – and have processes in place to address – financial regulations and HR directives, they also have a responsibility to themselves and any stakeholders to carefully manage their software assets and foster an appropriate level of awareness within their company.



¹ Source: GfK NOP "Commercial Risk" research, 2007

² Source: IDC "Software Piracy" study, 2007

This can seem challenging at first, especially if the organisation is growing quickly or there are substantial changes to the company structure. However, along with considering how best to work and communicate with stakeholders and employees, examining potential changes to financial status and reviewing contracts with suppliers and customers, time must be invested into managing software requirements. This will prove to be time well spent in the long term.

Well-implemented software management is not just about avoiding the risks to your business that unlicensed software use can cause, it can also deliver efficiency gains and significant cost savings; not only in terms of direct expenditure on software, but also in related process and infrastructure costs.

The benefits of effective software management are extensive: it can put you in a better position when negotiating with software providers and ensures you have the information you need to feel confident in your software purchasing arrangements.

It enables more strategic planning and prevents under and over-licensing, while reducing the IT administrative and support burden and its associated costs.

Your IT department or support services are better able to control what software employees have access to, including their ability to introduce unauthorised software on to your network.

The economic impact

Software piracy doesn't just have a negative impact on the business environment – there are far wider-reaching implications for the economy as a whole. Piracy drains revenues that software providers would otherwise invest in research and development, as well as jobs. Because software plays such a pivotal role in the information economy, this creates a ripple effect and impacts on other parts of the IT sector and the economy overall.

Not only does the IT industry employ hundreds of thousands of people and make a significant contribution towards GDP, it also drives productivity across most businesses. It is therefore vital that businesses recognise the value of software and ensure every piece is legal and properly licensed.

Best practice and a discerning approach to corporate social responsibility promote the idea of fair play and ethical behaviour in business, as well as the need to look after all the stakeholders in your company, including those companies that develop the software which is vital to your business.



Unlicensed software: what are the risks?

One-fifth of SMEs in Europe believe there is 'no risk' involved in installing, downloading or using unlicensed software, according to a study commissioned by the BSA³. However, there are many business risks inherent in this practice, and the assumption that there is no risk, and the belief that using unlicensed software is not something to be concerned about, is a worrying trend. Failure to understand the risks associated with unlicensed software can expose your business to numerous hazards.

The consequences of using unlicensed software can impact on a business from an operational, technical, financial, and legal perspective.



³ Source: GfK NOP "Commercial Risk" research, 2007

Operational and Technical Risks

Loss of & damage to data

Studies by IDC⁴ have found that pirated software, acquired via illegal downloads or counterfeit CDs, has a one in two chance of containing 'additional code'. Such as Trojans, viruses or spyware, that can crash IT systems or expose your confidential business data to intruders. In addition, pirated software may not offer security patches. In some cases only critical patches can be applied to unlicensed software. Downtime and security breaches can have immediate, negative effects on your bottom line.

Loss of functionality

In addition to the security risks of using pirated software downloaded from websites or P2P networks, such software is often sub-standard, or it can incur loss of functionality and compatibility issues that you would not encounter with legal, licensed versions. Unlicensed copies may not receive all updates from suppliers. This means your employees are unable to utilise the software fully, giving your competitors the edge – as they can respond more quickly, fully or effectively because they have the tools they require. There is also a risk that data becomes corrupted or is not saved correctly, leading to critical data loss.

Lack of technical support

With business operations relying so heavily on IT, it is critical that the relevant support systems are in place. Users of unlicensed software often don't have access to the crucial technical support provided by vendors and subsequently operate less efficiently.

Damage to reputation

Although difficult to quantify, the undeniable damage to the reputation of a business found operating with illegal software is a real risk – think about the impact if your customers aren't getting the level of service they expect. In fact, a survey carried out in the UK showed that 42% of people felt that if their customers knew they were using illegal software, they would be less inclined to do business with them.⁵

⁴Source: IDC "The Risks of Obtaining and Using Pirated Software" study, 2006

⁵Source: YouGov "Corporate Ethics" research, 2006

Financial and Legal Risks

Legal Penalties

Software development involves years of investment. It blends the creative ideas and talents of programmers, writers and graphic artists. Like most creative works, computer software is protected by copyright laws, and these laws must be respected by users in order for the software industry to continue to innovate.

When you purchase software, you don't become the owner of the copyright. Rather, by purchasing a licence, you become the copyright licensee with the right to use the software under certain conditions imposed by the copyright owner, typically the software publisher. The licence is a legal document, which defines the terms of use for any given software product. If a business breaches the terms of a software licence – such as copying, distributing or installing software in ways that the licence prohibits, whether intentionally or not – it is infringing the copyright and is breaking the law. Civil and criminal penalties vary across Europe, but significant fines can be levied.

Costs of being caught

If you are suspected of using unlicensed software the Business Software Alliance will take action. If you are found guilty of breaching software copyright legislation by having unlicensed software installed on company PCs. Your business will face paying substantial damages and legal costs. Your business will also have to purchase legal versions of the software it requires to continue to operate.

Fines

Depending on the sector you are in, unlicensed software use may lead to you facing fines from a variety of bodies – such as financial authorities, law enforcement or data protection bodies and so on. Many such bodies have criteria determining acceptable processes and such processes may be impacted by having unlicensed software – leaving your business open to additional financial penalties.

Costs of rectifying the problem

If caught with illegal software, businesses will often have to delete all unlicensed versions, meaning that they must replace the unlicensed software required with legal versions. It simply isn't worth taking this sort of a risk by cutting corners when it comes to software licensing, not to mention the disruption that could be caused to your business in dealing with a potential court case.

How does unlicensed software end up on your company's PCs?

Unlicensed software within business can derive from a variety of sources: unauthorised downloads by employees, hidden downloads via pop-up boxes launched by visiting some websites, and poor software licence management are just some. The causes of such lapses are often a lack of awareness amongst business executives and employees, inadequate IT policies, and poor software management processes. Unfortunately in some cases, use of unlicensed software is deliberate, with management fully aware of the situation, but still clearly unaware of the associated risks.

Approaches to combating the challenges identified below are discussed in the "How to reduce the risks" section.

Poor software and software licence management

Understanding the importance of software, the types of software available, and the different forms of software licensing can have a significant impact on how your business operates and expands, and therefore should be taken into consideration when making business decisions. By increasing awareness of the software assets within your organisation and ensuring they are managed and protected fully, they can be used more effectively to improve productivity and efficiency.

A variety of software licences are available for different requirements – from simple 'click-to-accept' formats to much more complex, negotiated arrangements. The flexibility continues to grow every year. Many standard licences allow for installation onto between one to five PCs, while volume licensing agreements typically allow a fixed number of installations to be made from a master CD. Any installations over and above the set levels must be agreed with your software publisher or reseller. All too often the absence of accurate records of installations or stringent company policies mean that companies can end up breaking the law.

Under-licensing occurs when software is used on more PCs than the licence allows, and is a common consequence of ineffective software and software licence management. If the licence allows the software to be installed on twenty desktops, any software installed on additional desktops is unlicensed – and breaches the terms of the licence. In effect it is an illegal copy and being caught with unlicensed software carries significant risks as outlined above.

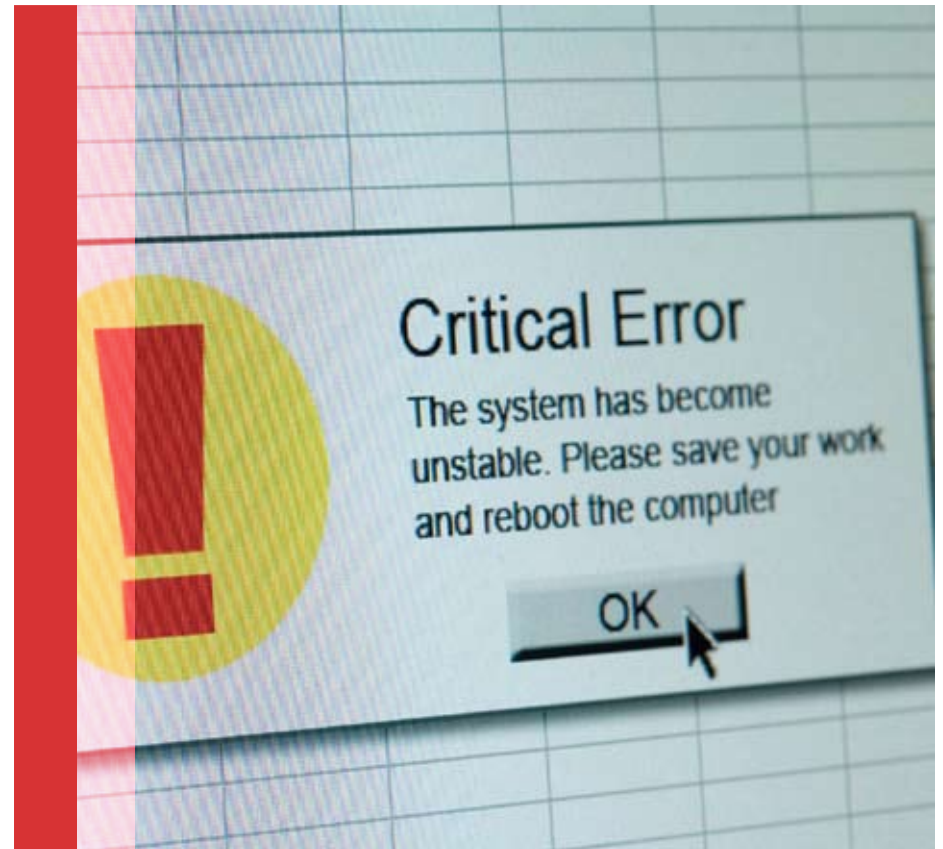
Downloads via the Internet

The Internet is an invaluable business tool, which many organisations rely heavily upon. Yet it also introduces the possibility of unwanted, unapproved software being downloaded onto company PCs unless appropriate checks and controls are in place.

As access to the Internet has become faster, it is far easier to purchase and/or download music, films and other multimedia. It has become increasingly simple for products to be moved from computer to computer with no hard media required and little risk of detection. Piracy that once required an understanding of complex computer codes can now take place with the click of a mouse.

Without blocking technology in place to prevent such unauthorised downloads, your business is vulnerable to employees downloading software without your knowledge or consent.

There are a number of risks inherent from this activity. If an employee has installed unlicensed software, the business owner or managing director is still responsible for the breach of copyright and the business can still face legal and financial risks. If the source of the software is not known, then the software downloaded could contain viruses, spyware or Trojans that have been given direct access to your IT networks.



There is also a growing risk from 'pop-up boxes' that appear on screen when an employee visits certain websites – often those offering 'bargain' software or images for download. Sometimes these act as a front for illegal activity and will install software, viruses or spyware onto the PC by tricking the employee into clicking on the pop-up itself.

Internet Auction Sites

One of the Internet's biggest successes has undoubtedly been auction sites. People are able to sell books, toys, collector's items, and even houses online. The flexibility, speed and success of such sites is testament not only to their popularity, but also the benefits they offer both to buyers and sellers. However, among the majority of honest and genuine offers are traps for the unwary buyer. The cheaper prices for seemingly genuine software mean they can be tempting for small and growing businesses keen to cut costs. However, the ability to hide or create false identities has led to many using this medium for illegal activity and auction sites have become a favoured vehicle for those looking to sell unlicensed or pirated software.

A study in 2006 by analysts IDC, actually revealed that less than 49% of Microsoft software offered on eBay was genuine.⁶

Once you realise you've bought illegal software, it can be very difficult to seek recompense. Of the 'duped' consumers who have registered complaints, very few have been reimbursed for their purchases. And of those who did receive money back – usually after devoting much time and effort to their claims – their refunds often didn't make up for the cost of their pirated items.

⁶ Source: IDC "The Risks of Obtaining and Using Pirated Software" study, 2006

Mobile working

Workforces across the world are becoming increasingly mobile, with employers equipping their staff with a variety of devices to work more efficiently when at home or out of the office. But with this increased freedom comes new challenges – the proliferation of devices used on the move and at home has increased the opportunities for staff to download illegal software onto their employers' networks. Your company is still liable for the software installed on laptops as they remain a corporate resource. The same applies for PCs employees may use at home, but which are owned by the employer.

Any Internet usage policies you have therefore need to include home use of company assets.

Bogus suppliers

There exists a small minority of software suppliers who bend the rules and knowingly sell illegal goods.

Many SMEs outsource the management of IT to external suppliers, so it is vital to carefully check the credentials of your software supplier.

Make sure your software supplier or reseller is able to satisfy for you that they are obtaining software from authorised distribution channels.

You can easily check authorised distribution methods by contacting software publishers directly and asking them who is authorised to distribute their products.

How to reduce the risks

There are a number of steps your business can take to minimise the risks posed by unlicensed software.

Regular Audits and Effective Usage Policies

This is not a 'technology issue' but a business issue, which can often be resolved through business best practice. Given the risks, getting buy-in at a business level for certain processes to be put in place is key.

At the very least every business should regularly audit the software that is installed on its PCs, and should have employee policies in place with regards to accepted usage of company technology (including technology used at home or mobile technologies used by the employee but owned by the business). It should be made clear that the policies will be enforced and, where possible, those responsible for personnel should be involved to ensure success.

Software Asset Management

Surprisingly, one third of SMEs have not heard of Software Asset Management.⁷

Software Asset Management (SAM) is a methodology that assists businesses in defining and implementing processes to optimise their investment in software. Flexible enough for businesses of all sizes and at any stage of development to utilise, SAM can identify where your business may be vulnerable to the risks discussed above and ensure processes are in place to mitigate or prevent you falling victim to such risks.

SAM involves bringing together employees, processes and, where required, technology to ensure software assets are managed, protected, and utilised as effectively and efficiently as possible. In addition, licences and usage are systematically tracked, evaluated and managed. The business benefits of SAM can be significant: besides giving you peace of mind, it can help to reduce IT expenditure as organisations can accurately plan and budget their software requirements, including new software and licence upgrades.

To develop SAM effectively within your business there are a number of steps you can take. You don't have to bring all these elements into play from the start – each one will bring some improvements – but recognition that software is a critical business asset, and its management a key business issue must be the starting point.

⁷Source: GfK NOP "Commercial Risk" research, 2007

Eight Steps to Implementing Software Asset Management:

1 Get company-wide support

Implementing SAM means a significant cultural change – it is vital to ensure that both senior management and end users support the project and understand the need for SAM.

2 Appoint a software asset manager

Unless you have one person overseeing software throughout a company, it is very difficult to keep track of software assets. This does not have to be someone in the IT department but, depending on the size of your organisation, the person who is responsible for IT administration (and therefore has involvement in software purchasing) is best. If you only have one person with responsibility for IT – often the case in smaller firms – make it a clear and defined part of their job description.

3 Audit current software and licence usage

You will need to take an inventory of your current software assets in order to know exactly what software is running in your company and the licences required for this software.

Only by knowing what software is installed, how many computers your organisation has, and whether there are any copies of programmes that may have been installed by employees, are you in a position to identify potential risks or issues and take measures to counteract them.

4 Create a software asset management database

Having a good database to store all information regarding your software is vital to the success of your SAM strategy. You could use a spreadsheet or invest in something designed for the task – either way it will prove invaluable.



5 Centralise the purchase and distribution of your software

If there is no single view of software spending or purchase responsibilities, it will be nearly impossible to realise the full benefits of SAM.

6 Set policies and procedures

Controlling how software gets into your company is one of the best preventative measures you can take. A clear and enforced employee policy statement covering what is and isn't allowed will help keep the situation under control.

Ensuring that staff fully understand and buy into your software asset management strategies will mean that you are one step closer to controlling the environment in which software is introduced into your organisation.

7 Monitor Regularly

Be aware that SAM is a continual process and will require monitoring through regular audits in order to function smoothly and efficiently.

8 Use an impartial advisor for help

To help businesses wanting to avoid the risk of unlicensed software, the Business Software Alliance has created an online resource on its website (www.bsa.org), which provides advice and Software Management tools. Just visit the Tools and Resources site to find out more.



What if you think you may be at risk?

Businesses should treat software like any other valuable asset. By taking action and implementing the suggestions listed here, you can manage the business risks associated with illegal software and reap the benefits of a more efficient IT environment.

If, however, you are worried that your company is at risk from illegal software, there are a number of bodies that can be contacted for help. Resellers and vendors should be the first port of call to answer any questions you may have regarding software licences.

Other tools available on the BSA website include:

1

Guide to Software Management and Licensing:

Brochures available for download in seven languages that help businesses implement software management procedures and clarify licensing compliance.

2

List of Resource Management Providers:

A list of links to major software suppliers and consultants that can assist companies with licensing and the implementation of software management programmes.

Conduct a free online Healthcheck

The Healthcheck tool was developed by the BSA to help businesses identify, understand, and manage IT assets in a more effective manner. In a few minutes it can:

1. Conduct an analysis of your current software management position
2. Highlight areas of potential vulnerability
3. Recommend improvements
4. Generate a tailored Healthcheck report for your records

<http://global.bsa.org/healthchecktool>

Appendix: Key Findings from the Gfk NOP Research

In 2007, the BSA commissioned a European-wide study to investigate SME attitudes to software piracy, and whether there is a good understanding of the risks involved in operating a business with illegal software.

1 94% of European SMEs claim IT is 'Very' or 'Fairly' important to their businesses ability to operate successfully.

2 Across Europe (not including Russia) one-fifth of respondents believe there is 'no risk' from using unlicensed software.

3 87% do not realise using illegal software could make them more vulnerable to viruses.

4 97% do not consider having to use old versions of software due to an inability to upgrade from illegal versions a problem.

5 The most common risk cited by respondents is 'criminal proceedings' (23%), followed by 'financial penalties' (21%). Only 3% stated that 'having to run old versions/inability to upgrade' was a risk – despite the commercial threat of competitors having the latest solutions.

6 However, twice as many SMEs in Central and Eastern Europe and Russia refer to 'loss/damage to data' as a risk of using unlicensed software compared to Western businesses, and in Russia 'software failure' was seen as a risk by 27% but only 8% of Western business people shared this view.

7 Larger SMEs (100 – 250 employees) are more likely to have some form of process to manage the use of software in place (37%) compared to smaller SMEs (19%).

8 Overall 'regular audits of staff PCs' is the favourite method of controlling and managing software usage (33%), with 'company policy' coming second (25%).

The Research

The research was conducted on behalf of the BSA by Gfk NOP via telephone with 1,800 small and medium-sized enterprises across Europe in UK, France, Germany, Netherlands, Italy, Spain, Russia, Poland and Hungary.

200 interviews were conducted in each of the regions. For the purposes of this research, SMEs were defined as enterprises with between 10 and 250 employees.



BSA Worldwide Headquarters

1150 18th Street, NW
Suite 700
Washington, DC 20036
USA
Phone: +1 202 872 5500
Fax: +1 202 872 5501

BSA Europe, Middle East, and Africa

2 Queen Anne's Gate Buildings
Dartmouth Street
London SW1H 9BP
United Kingdom
Phone: + 44 (0) 20 7340 6080
Fax: + 44 (0) 20 7340 6090

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555
Phone: + 65 6292 2072
Fax: + 65 6292 636

<http://www.bsa.org>

The Business Software Alliance (BSA) is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce.

BSA, Business Software Alliance and the BSA logo are trademarks of the Business Software Alliance Incorporated and may be registered in certain jurisdictions.
© 2007 Business Software Alliance. All rights reserved.