ISO 27001 Global Report
2015

96% of respondents say that ISO 27001 plays an important role in improving their company's cyber security defences

www.itgovernance.co.uk

Introduction

Cyber attacks are increasing in frequency, severity and number, seriously damaging the reputations of some organisations and threatening the very existence of others. It is therefore unsurprising that information security is now a top business priority.

While new stories of breaches and threats emerge on a daily basis, less attention is paid to the critical measures that businesses should adopt in order to reduce the likelihood of suffering a data breach.

This report aims to put the focus back on the fundamentals of cyber security, which we firmly believe are underpinned by ISO 27001.

Information security and ISO 27001

Over the past ten years, the popularity of ISO 27001, the international best-practice information security management standard, has increased significantly: the most recent annual ISO survey[i] shows that certifications to the Standard have been growing steadily year-on-year. The latest figures show a 14% increase on the previous year (reflecting 22,293 certificates issued globally in 2013).

As a company whose main focus is cyber security and ISO 27001, IT Governance has closely witnessed the growing popularity of the Standard from its early days in 1995 (when it was known as BS 7799) to the present day. While many organisations are yet to realise the benefits and importance of ISO 27001, we are delighted that thousands of companies have embraced the Standard to better protect their corporate data.

The value of ISO 27001 to any business lies in the fact that it is, first, a management standard and, second, that it looks at information security from a holistic point of view. ISO 27001 encompasses people, processes and IT systems, in recognition that information security is not just about antivirus software, but depends on the effectiveness of organisational processes and the people who manage and follow them. Implementation of the Standard provides organisations with a strategic as well as operational approach to information security, enabling them to prioritise, integrate and cross-reference different initiatives to ensure overall effectiveness.

[i] *www.iso.org/iso/iso-survey*

About IT Governance

IT Governance is a leading global provider of IT governance, risk management and compliance solutions, with a special focus on cyber resilience, data protection, PCI DSS, ISO 27001 and cyber security.

Having led ISO 27001 implementations since the inception of the Standard, our strong global cyber security presence gives us the knowledge and insight to provide valuable advice, tailored to meet any organisation's specific needs or budget.

More information is available at www.itgovernance.co.uk.

The ISO 27001 survey

As global experts on ISO 27001 implementation with an impressive track record of hundreds of projects delivered globally, we felt it appropriate to undertake our own research to explore the challenges and drivers behind the Standard's increased adoption. To the best of our knowledge, there hasn't been any recent similar research undertaken globally, which makes our survey all the more valuable.

It gives us a great pleasure to present the results of research that was carried out between December 2014 and January 2015.

We are grateful to the 245 respondents who took the time to answer our questions. While the majority of contributions come from the United Kingdom (45%), the United States (9%) and India (9%), 37% of the respondents are based in other parts of the world, including Australia, South America, Africa, Europe and Asia. The sample of industries is also very broad and includes businesses services, financial services, manufacturing, technology, and telecommunications. Moreover, the respondents come from enterprises of different sizes – a clear demonstration that ISO 27001 is applicable to any organisation.

We believe that the findings of this report provide a real insight into the uptake of ISO 27001. They contain clear evidence of the business benefits of ISO 27001 implementation, which makes us confident that more organisations will be encouraged in the future to turn to international best practice when devising their information security plans.

Finally, we would like to urge the readers of this report to carefully review the challenges that are associated with the implementation of ISO 27001 and to devote special effort and resources to addressing them in order to achieve the best for their organisations.

The IT Governance team

Alan Calder
Founder and Executive Chairman of IT Governance

Steve Watkins
Director, IT Governance

Alan Calder and Steve Watkins led the world's first successful implementation of BS 7799 (now ISO 27001).

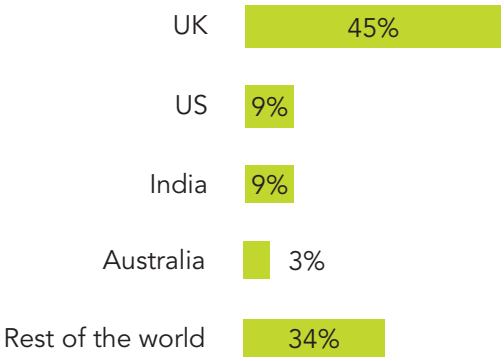
They have co-authored the definitive compliance guide, IT Governance: An International Guide to Data Security and ISO27001/ISO27002 (now in its fifth edition), which is the basis for the UK Open University's postgraduate course on information security.

Contact us:

T: +44 (0)845 070 1750
E: servicecentre@itgovernance.co.uk

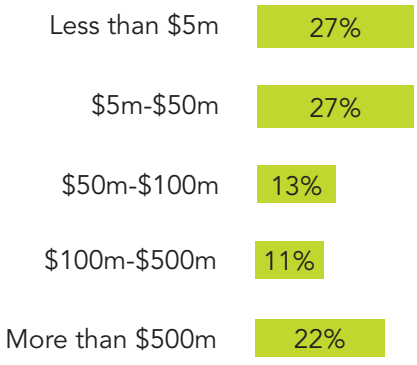
Survey participants

By country

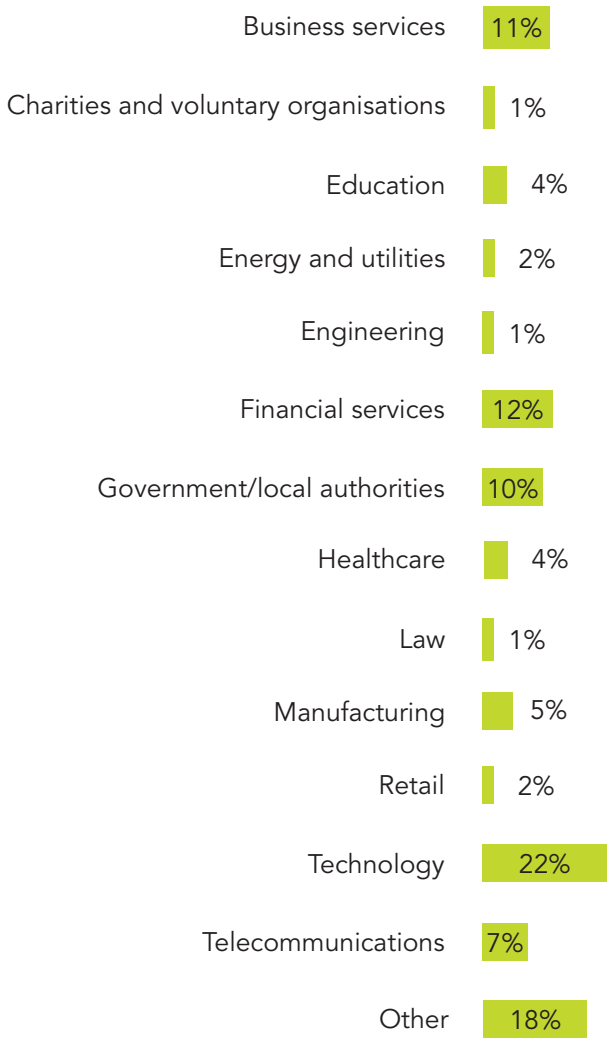


By size of organisation

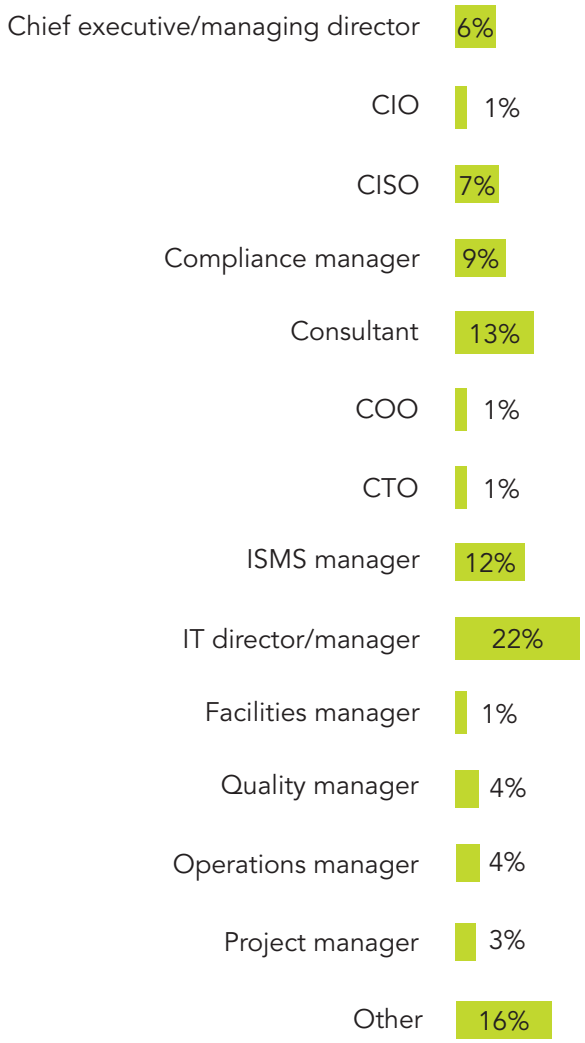
By company revenue (US$)



By industry sector



By job title



Key findings at a glance

ISO 27001 certification is the norm

84% of organisations that have implemented an ISO 27001-compliant information security management system (ISMS) have achieved or are working towards certification to the Standard.

Information security is the most important driver for and benefit of ISO 27001 implementation

Nearly 70% say that improving information security was the biggest driver for implementing ISO 27001, followed by the requirement "to align with information security best practice" (62%) and "gaining a competitive advantage" (57%). Improved information security is also seen as the single most important benefit of ISO 27001 implementation (51%).

ISO 27001 plays an important role in improving an organisation's cyber security defences

A whopping 96% of respondents agree that ISO 27001 plays an important role in improving their company's cyber security defences.

CEOs support ISO 27001 implementation

More than a third (38%) of respondents reported they had no challenge securing their board or CEO's buy-in when implementing ISO 27001. Only 20% found it a challenge "convincing the board that information security is a critical business issue".

Appropriate expertise and staff awareness are the two biggest challenges when implementing ISO 27001

45% of respondents admitted that "obtaining employee buy-in and raising staff awareness" is one of the biggest challenges when implementing ISO 27001, followed by assembling "the right level of competence and expertise" (44%) and "securing the required budget" (33%).

Asset-based risk assessment is the most common risk methodology

An asset-based risk assessment is the most common risk methodology (31%). 20% of respondents state that their risk assessment methodology "has historically been and will continue to be asset-based", while 11% indicated that their risk assessment methodology is a new initiative and will be asset-based. 20% will use a combination of asset and scenario-based methodologies.

Key findings at a glance (continued)

The security controls provided in ISO 27001:2013 are the most popular

77% of respondents use the security controls provided in Annex A of the 2013 version of the Standard, while 19% are still making use of controls from Annex A of ISO 27001:2005. 21% of respondents use PCI DSS controls, and 4% employ the Cloud Controls Matrix.

ISO 27001 plays an important role in customer and supply chain assurance

Two-thirds of organisations have been asked by their clients about their ISO 27001 status in the past 12 months, while 44% have asked their suppliers for ISO 27001 certification in the same period.

Only 23% employ a dedicated, full-time ISMS manager

Only 23% of respondents state that their company employs a full-time ISMS manager. It is worth noting that 24% of organisations have made a C-level position (CISO, CIO or CTO) responsible for the ISMS. 10% of organisations have assigned the management of their ISMS to a compliance manager.

44% of organisations employ ISMS managers who don't have a formal ISO 27001 ISMS qualification

Worryingly, 44% of respondents admitted that the person managing their ISMS doesn't have a formal ISO 27001 ISMS qualification. Despite this lack of relevant training, 28% are not planning to train the personnel managing their ISMS, while 35% do not have control over that decision.

40% of organisations seek external help for certification

40% of organisations have sought external help for certification. The lack of a full-time ISMS manager as well as a shortage of formal training for those managing the ISMS may be the factors contributing to this trend.

The majority of organisations achieve certification within 6 to 12 months of the start of the project

47% of those who have achieved ISO 27001 certification say it took them between 6 and 12 months to achieve certification. Only 5% took longer than 24 months to achieve certification.

The benefits of ISO 27001 certification fully justify the investment

68% of respondents say that certifying to ISO 27001 is an investment that is fully justified by the benefits.

Finding 1

ISO 27001 certification is the norm

40% of organisations have achieved ISO 27001 certification and 44% are working towards achieving certification. Only 16% are not planning to certify their ISMS.

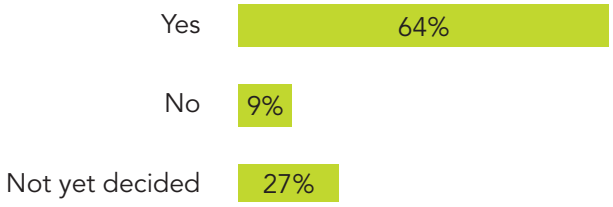
It is unsurprising that such a large percentage of organisations pursue certification to ISO 27001. Since its first publication in 1995, when it was called BS 7799, ISO 27001 has evolved as the internationally recognised best practice for information security management.

Certification to the Standard not only boosts an organisation's security, but also demonstrates to stakeholders and other third parties that this is the case by showing that the organisation has passed an external, independent audit.

The fact that more and more organisations are choosing the certification route is also confirmed by ISO's latest annual survey, which reveals that the number of certificated organisations is growing consistently year on year: the global annual certification growth rate was 14% at the end of 2013.

Have you achieved ISO 27001 certification?

If you have been certified, are you still continuing to renew your certification every three years?



Finding 1 (continued)

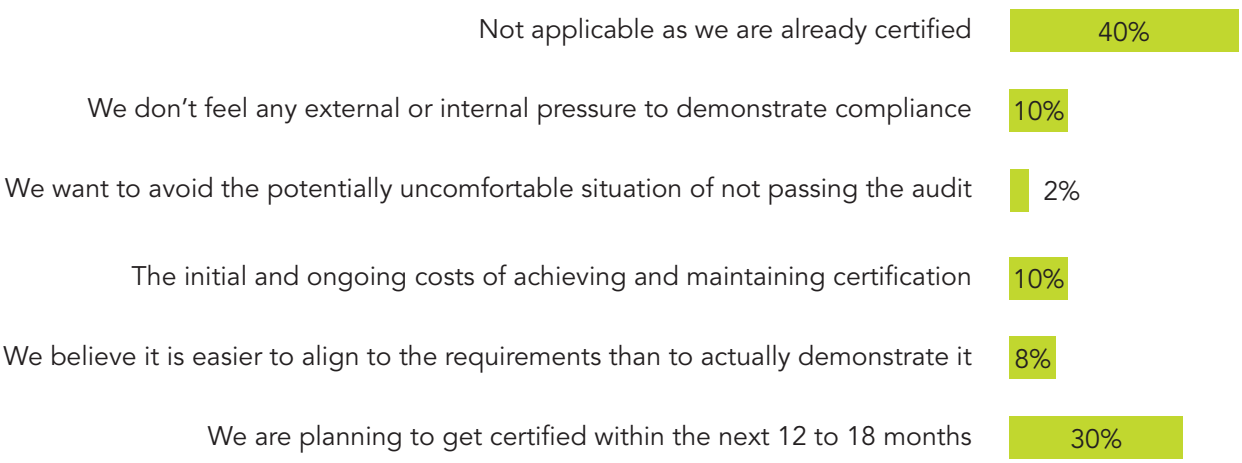
The "initial ongoing costs of achieving and maintaining certification" (10%), and a lack of "external or internal pressure to demonstrate compliance" (10%) are the main reasons that some organisations don't pursue certification.

8% of respondents believe that it is easier to align with the Standard's requirements than to demonstrate compliance by achieving certification. 2% cited fear of embarrassment about not passing the audit as an obstacle to achieving certification.

64% of organisations continue to renew their certification every three years and 27% are yet to make a decision. Only 9% choose not to recertify.

An accredited ISO 27001 certificate is valid for three years, after which the certified organisation must undergo a recertification audit. Throughout the three-year certification period, the organisation is subject to surveillance visits by its chosen certification body to check that it is maintaining and continually improving its ISMS.

If you have implemented ISO 27001, but haven't certified to it, what is the main reason your company will not proceed with achieving certification to ISO 27001?



Finding 2

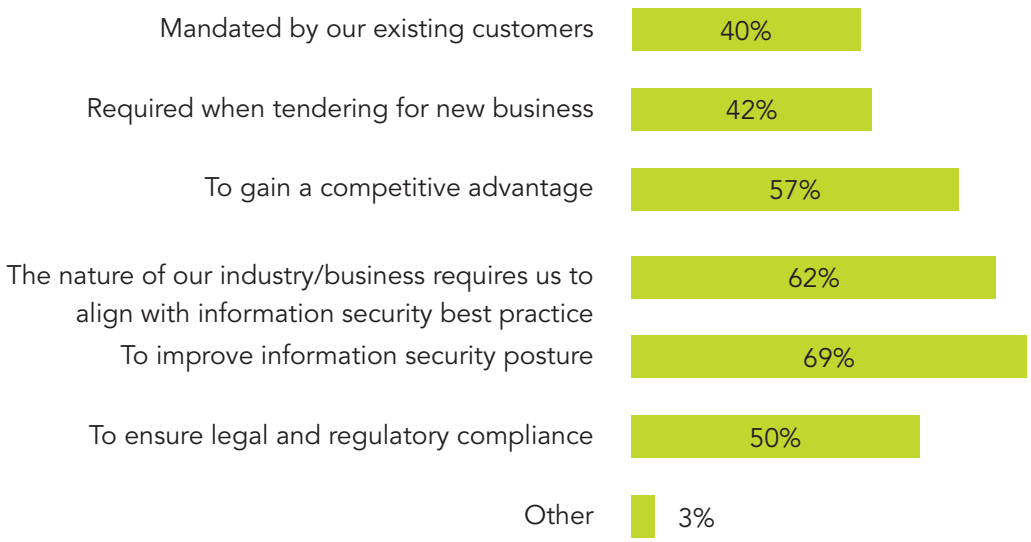
Information security is the most important driver for and benefit of ISO 27001 implementation

69% of respondents said that improving the information security posture of their organisation was the biggest driver for ISO 27001 implementation.

Meeting industry requirements to align with information security best practice is the second most important driver (62%) and gaining competitive advantage is the third (57%).

Other key drivers include ensuring legal and regulatory compliance (50%) and fulfilling tender requirements (43%). 40% stated that their clients mandate ISO 27001 compliance.

What are the main drivers for implementing ISO 27001 in your organisation(s)?[i]



[i] *Respondents could chose more than one answer.*

Finding 2 (continued)

When it comes to the benefits of ISO 27001 implementation, more than half of the respondents (51%) pointed at "improved information security across the whole organisation" as the single most important benefit.

12% of respondents believe that they have benefited most from an improved company image and reputation, followed by 10% who have gained most from improved internal processes. 7% believe that ISO 27001 has helped them create new business opportunities and another 7% see improved staff awareness of information security as the biggest benefit.

Other benefits include improved competitiveness (6%), retention of existing clients (3%), the reduced cost of data breaches (2%) and improved profitability (1%).

The fact that there are so many different benefits to implementing the Standard highlights that ISO 27001 adds true business value by underpinning so many different areas of the business.

These responses should be of particular interest to organisations that haven't embraced the Standard yet because of uncertainty about the return on investment. These findings undoubtedly support and strengthen the case for ISO 27001 implementation and certification.

What is the single most important benefit that ISO 27001 implementation has brought or will bring to your organisation?

Finding 3

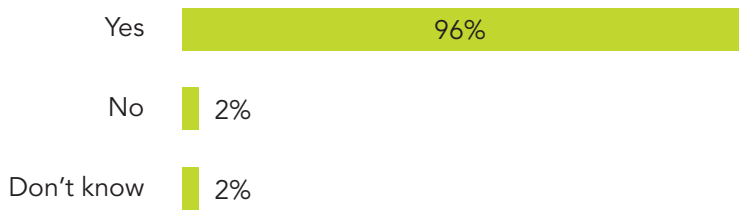
ISO 27001 plays an important role in improving an organisation's cyber security defences

96% of respondents agree that ISO 27001 plays an important role in improving their company's cyber security defences. This is in line with Finding 2 and highlights the significance of the Standard for today's businesses.

ISO 27001 requires that information security management decisions are entirely driven by the outcome of a risk assessment in relation to identified risks. The risk assessment enables expenditure on controls to be balanced against the business harm likely to result from security failures.

As the ISO 27001-determined controls used are based on the outcome of a risk assessment and the risk acceptance level set by management, an ISMS offers the opportunity to define and monitor risk levels internally – as well as in contractor/partner organisations – by demonstrating the extent to which there is effective control of the risks for which directors and senior management are accountable.

Do you believe that ISO 27001 plays or will play an important role in improving your company's information security defences?



Finding 4

CEOs are supportive of ISO 27001 implementation

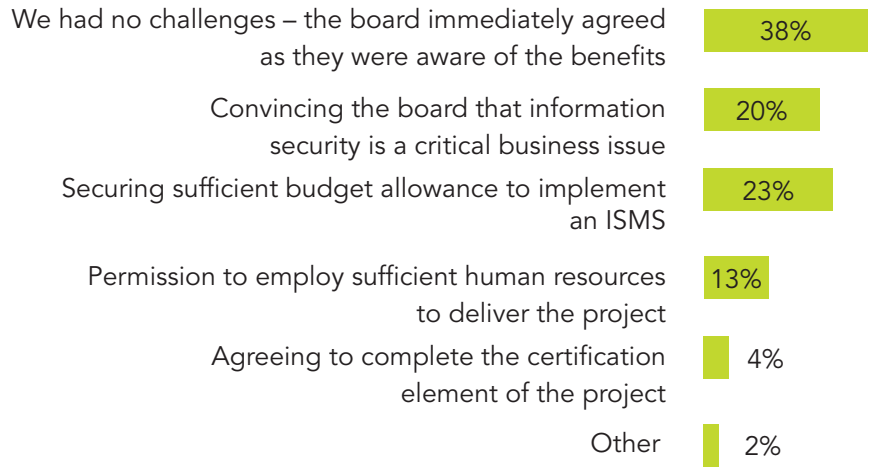
38% of respondents state they had no challenge securing their board or CEO's buy-in when it came to implementing ISO 27001. For 23%, securing sufficient budget to implement an ISMS was the biggest challenge, compared to 20% who found it most challenging to convince the board that information security is a critical business issue.

A further 13% struggled to secure permission to employ sufficient human resources to deliver the project and 4% found their biggest challenge was obtaining the board's approval to complete the certification element of the project.

The fact that more than a third of CEOs support the implementation of ISO 27001 may be because of the growing awareness of the importance of information security among senior management. This statistic will undoubtedly encourage information security professionals who are yet to put the case for ISO 27001 to their boards.

An ISO 27001-compliant ISMS encompasses people, processes and technology, and necessarily affects the whole organisation. A top-down approach is therefore critical to the implementation project's success.

What do you consider has been or will be the biggest challenge to securing your board's/CEO's buy-in to implement ISO 27001?



Finding 5

Competence and staff awareness are the two biggest challenges when implementing ISO 27001

45% of respondents admit that obtaining employee buy-in and raising staff awareness are the biggest challenges when implementing ISO 27001. 44% reported that ensuring they had the right level of competence and expertise was the biggest challenge, and 33% were challenged by securing the required budget (33%). Conducting the information security risk assessment is ranked the fifth most challenging aspect of ISMS implementation, at 30%.

Other main challenges include identifying the required controls (20%), mobilising the ISO 27001 implementation team (19%), developing the scope (18%) and obtaining certification to the Standard (14%).

What would you consider the main challenges when implementing ISO 27001?

Finding 5 (continued)

Implementing an ISO 27001-compliant ISMS is a complex undertaking that involves the whole organisation. The knowledge and experience of those responsible for the implementation is fundamental both to the success of the project and to the long-term effectiveness of the ISMS. Therefore, organisations shouldn't shy away from investing in professional staff training and calling upon external experts in order to complete the project successfully within the timeframe they have set.

Additionally, increasing awareness among non-technical staff is essential – it is a well-known fact that employees are the weakest link when it comes to information security. Ensuring that staff understand the benefits of ISO 27001 and the threats to their and the organisation's information will help secure their buy-in in the project.

Finding 6

Asset-based risk assessment is the most common risk methodology

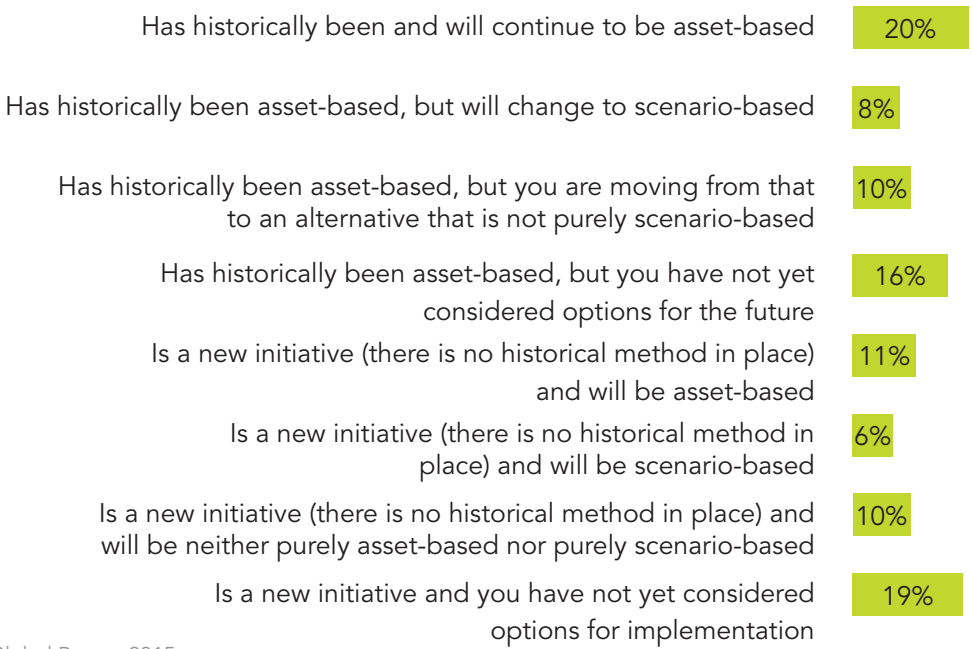
The risk assessment requirements of ISO 27001:2013 are less prescriptive than those of the 2005 version. ISO 27001 no longer mandates an asset-based information security risk methodology, but provides more flexibility in the method that organisations can apply.

With 31% of respondents following an asset-based risk assessment, it is currently the most common risk methodology – 20% of respondents state that their risk assessment methodology has historically been and will continue to be asset-based, while 11% indicated that it is a new initiative and will be asset-based.

However, things may change: 16% of respondents state that they are yet to consider options for the future. 19% have not yet decided as they are in the early stages of implementation and 10% are moving from an asset-based to an alternative methodology that will blend asset- and scenario-based approaches.

Another 10% will be deploying neither purely asset-based nor purely scenario-based risk assessment methodologies. 8% of respondents have been performing asset-based risk assessments, but are planning to change to scenario-based ones, and 6% will use the scenario-based approach.

ISO 27001:2013 is more flexible than the 2005 version regarding the information security risk methodology. Your ISO 27001:2013-aligned information risk methodology:



Finding 6 (continued)

The risk assessment process sits at the core of ISO 27001. The accuracy of the risk assessment is critical as its outcome drives information security management decisions.

It is interesting to note that the asset-based assessment methodology remains popular, with most organisations planning to use either an asset-based approach, or a blend of asset- and scenario-based approaches.

We recommend using a risk assessment software such as **vsRisk™** to simplify and accelerate the risk assessment process and follow the proven ISO 27005 risk assessment approach.

Find out more:
www.itgovernance.co.uk/shop/c-333-software.aspx

Finding 7

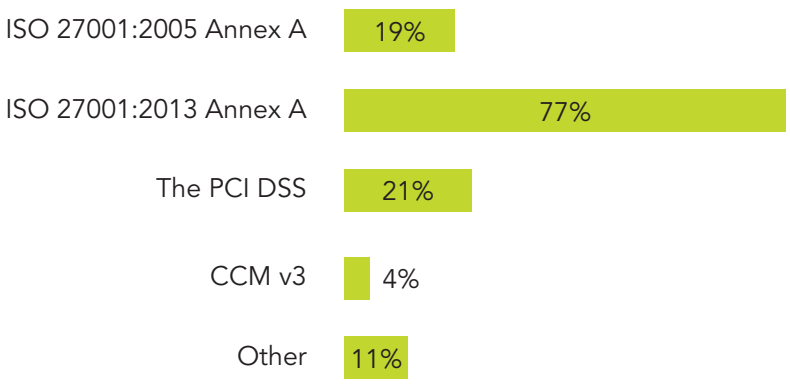
The security controls provided in ISO 27001:2013 are the most popular

ISO 27001:2013 requires organisations to determine controls "from any source", which should then be compared with those in Annex A to ensure that no necessary controls have been omitted.

77% of respondents state that they have selected or will select their security controls from Annex A of ISO 27001:2013, compared to 19% who have selected or will select the controls from Annex A of ISO 27001:2005. 21% have selected or will select their security controls from the PCI DSS and 4% from CCM v3.

The selection of controls is a core element of ISO 27001. The Standard requires an organisation to determine the information security processes and controls that need to be monitored and measured in order to evaluate the performance and effectiveness of the ISMS. The selection of the necessary controls is determined by the outcome of the risk assessment and the risk treatment plan.

Security Control Set – ISO 27001:2013 requirements provide the option to select a security control set other than Annex A. Which of the following have you selected/will you select your security controls from:



Finding 8

ISO 27001 plays an important role in customer and supply chain assurance

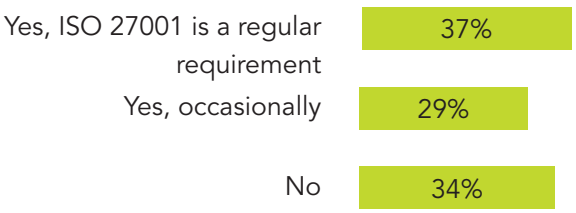
Two-thirds (66%) of organisations have been asked by their clients about their ISO 27001 status in the past 12 months. More than half of those reveal that ISO 27001 is a regular requirement for contracts and tendering for new business, while the others state that they have been asked occasionally.

In contrast, only 44% of respondents have asked their suppliers for ISO 27001 certification in the past 12 months. 39% haven't asked their supply chain for ISO 27001 certification and 17% don't know.

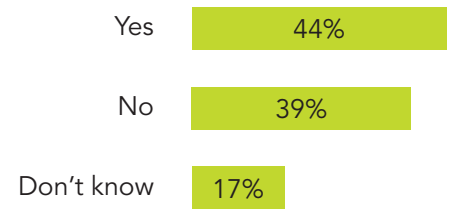
Few organisations do not rely on suppliers, so it is vital that senior executives become more insistent about information risk assurance with their suppliers and trading partners. Suppliers are often an attractive target for hackers as they can provide an easy way in to larger organisations. Many recent high-profile data breaches, including those affecting Target and Home Depot, involved a supplier.

If suppliers are going to have access to a company's data, networks or systems, it is essential that they are subject to at least the same level of security as the company procuring their services.

Have any of your customers enquired about your ISO 27001 status in the past 12 months?



Have you asked your suppliers for ISO 27001 certification in the past 12 months?



Finding 9

Only 23% of organisations employ a dedicated, full-time resource to manage their ISMS

Only 23% of respondents state that their company employs a dedicated, full-time ISMS manager. The rest delegate this activity to various other roles within the organisation. Unsurprisingly, IT managers head this group, with 22% tasked with ISO 27001 implementation. In some organisations, the ISMS is overseen by C-level positions, including CISOs (14%), CIOs (8%) and CTOs (2%).

10% of organisations delegate their ISMS management to a compliance manager, 4% to a quality manger and 4% to a project manager.

This suggests that more than two-thirds of organisations are stretching their internal resources by expecting their ISMS to be managed by someone in addition to their core duties. It also explains to some extent why 44% see competence and expertise as a big challenge (Finding 5).

Competence is essential for the planning, implementation, maintenance and auditing of an effective ISMS. Whether the company employs a full-time ISMS manager or has tasked another role with the project, formal training and qualifications are necessary to ensure the quality of the ISMS and to provide return on investment.

Who manages the ISMS in your organisation?

Finding 10

44% of those responsible for the ISMS don't have a formal ISO 27001 ISMS qualification

44% of respondents admitted that the person managing their ISMS doesn't have a formal ISO 27001 ISMS qualification. Despite this lack of relevant training, 28% are not planning to train their ISMS manager, while 35% do not have control over that decision.

Closely related to findings 5 and 9, these statistics paint a worrying picture. Despite a lack of skills and expertise, only 37% of organisations are planning to train existing ISMS managers.

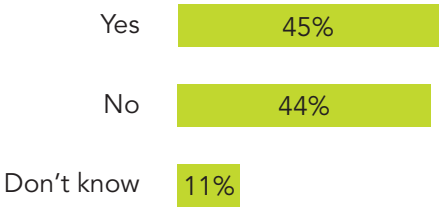
The proliferation of cyber attacks and data breaches, together with the deepening cyber security skills shortage, should alert companies to the dangers of neglecting internal skills and expertise. Given the importance of this issue, businesses should be investing more in improving cyber security education within the organisation rather than shrinking their training budgets. Providing staff with the necessary knowledge and skills to manage the company's ISMS effectively is the best way to tighten cyber security, successfully achieve ISO 27001 certification and get return on investment.

Moreover, the Standard requires that sufficient resources are available to work on the ISMS and that all employees affected by the ISMS have the proper training, awareness and competency.

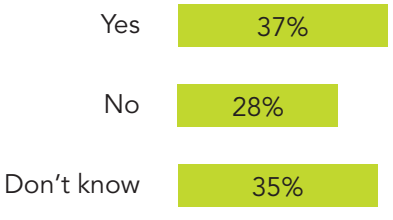
IT Governance is well known for its comprehensive **ISO 27001 course portfolio**, which provides organisations with the internal skills to achieve compliance. It also helps individuals advance their career through a structured qualification scheme.

Find out more:
www.itgovernance.co.uk/iso27001-information-security-training.aspx

Does the person managing your ISMS have a formal ISO 27001 ISMS qualification (e.g. ISO 27001 Lead Implementer or ISO 27001 Lead Auditor)?



Are you planning to formally train the person managing your ISMS to officially recognised ISO 27001 qualifications?



Finding 11

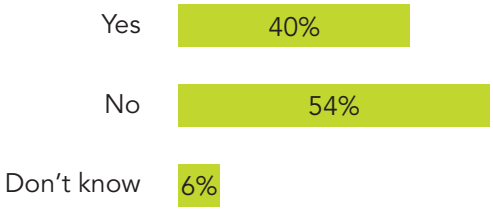
40% of organisations seek external help for certification

40% of organisations have sought external help for certification. The absence of a full-time ISMS manager as well as a shortage of formal training for those tasked with ISMS management (see Finding 10) may contribute to this trend.

A lot of SMEs that don't have an ISMS manager or even an IT manager would benefit from using external help when implementing ISO 27001.

It is worth noting that large organisations with a dedicated ISMS manager could still benefit from external help and advice as ISO 27001 implementation is usually much more complex for them, especially if it involves several locations. Mobilising internal experts and calling in external help can considerably accelerate a project, especially if there is a tight deadline.

Have you used external consultants to help you prepare for certification?



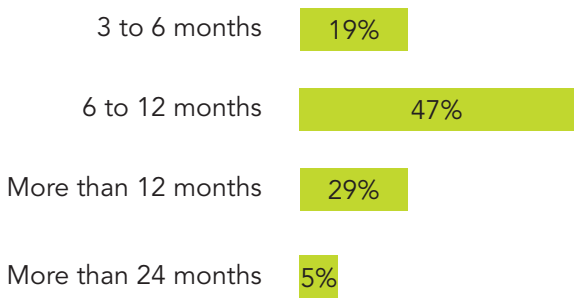
Finding 12

The majority of organisations achieve certification within 6 to 12 months from the start of the project

47% of those who have achieved ISO 27001 certification, say it took them between 6 and 12 months to do so. Only 5% of respondents took longer than 24 months to achieve certification. 19% did it in more than 12 months and 29% succeeded within three to six months.

The time it takes to achieve ISO 27001 certification can vary depending on the size of the organisation, the scope of the project and the availability of resources. For example, small companies with a single office location and few members of staff may be able to achieve certification in less than three months if they rely on external help. Larger organisations will take longer, but this will also depend on their internal structure, existing practices, project plan and resource schedule. Taking into account Findings 9 and 10, the project duration is also closely related to the availability of a dedicated ISMS manager and the skills and experience of the person responsible for the project.

How long did it take your organisation to achieve certification from the start of the project?



Finding 13

The benefits of ISO 27001 certification fully justify the investment

68% of respondents would characterise certifying to ISO 27001 as "an investment that is fully justified by the benefits".

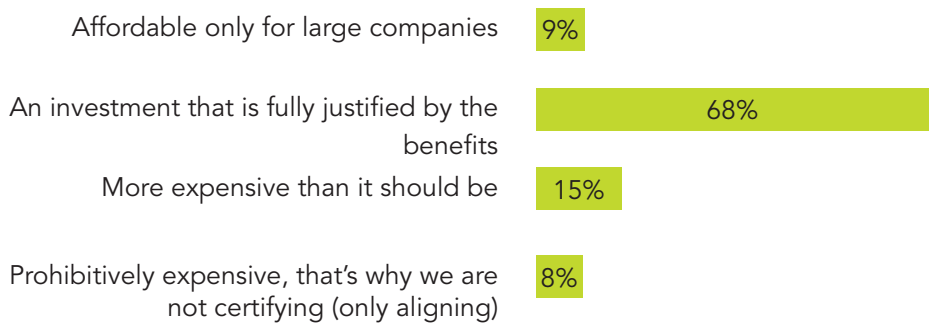
15% of respondents believe certification is more expensive than it should be, while 9% perceive certification as affordable only to large organisations. 8% consider the expense prohibitive and therefore are not certifying to the Standard, but only aligning with its requirements.

The fact that such a high percentage of respondents believe that ISO 27001 certification is justified by its benefits clearly speaks of the business value of the Standard – also see Finding 2.

IT Governance's annual **ISMS Management Service** helps you to proactively manage, monitor and maintain your information security management system (ISMS), ensuring consistent conformity to ISO 27001.

Find out more:
www.itgovernance.co.uk/shop/p-1673.aspx

Would you characterise certifying to ISO 27001 as (please choose one option):



Looking to implement or achieve certification to ISO 27001?

Leverage our ISO 27001 expertise 24/7 to protect your information assets anywhere in the world. Our unique structured solutions enable any organisation to **implement ISO 27001 at a speed and for a budget that is appropriate** to their individual needs and preferred project approach.

Find out more: www.itgovernance.co.uk/iso27001-solutions.aspx

What is included?	The Basics	Do It Yourself	Get A Little Help	Get A Lot Of Help	We'll Do It For You
ISO 27001:2013 (standard PDF)	✓	✓	✓	✓	FastTrack™ Service
ISO 27002:2013 (standard PDF)	✓	✓	✓	✓	
ISO 27000:2014 (standard PDF)	✓	✓	✓	✓	
Nine Steps to Success (eBook)	✓	✓	✓	✓	
IT Governance: An International Guide to Data Security (eBook)	✓	✓	✓	✓	
ISMS Standalone Documentation Toolkit		✓	✓	✓	Bespoke Solution
vsRisk - Risk Assessment Software		✓	✓	✓	
Lead Implementer Online Training			✓	✓	
Lead Auditor Online Training			✓	✓	
Online Consultancy			**2 hours**	**5 days (with a mentor)**	

Additional ISO 27001 resources

At IT Governance we provide unique products and services that cover every aspect of information security and ISO 27001 – ranging from books, toolkits, guides, training courses and consultancy to ISO 27001 audits.

To view our full offering, visit www.itgovernance.co.uk/shop and select ISO 27001 from the menu.

Standards & Management Frameworks	Books & Guides	Toolkits	Software
ISO 27001:2013	ISO 27001 Nine Steps to Success	ISO 27001:2013 Gap Analysis Tool	vsRisk™ Information Security Risk Assessment Tool
ISO 27002:2013	The Case for ISO 27001	ISO 27002 Controls Gap Analysis Tool	ISO 27001 Compliance Database
ISO 27032:2012	An Introduction to Information Security & ISO 27001 Pocket Guide	ISO 27001:2005 to ISO 27001:2013 Conversion Tool	Information Classification Software
ISO 27005:2011	ISO 27001 & ISO 27002 Pocket Guide	ISO 27001:2013 Toolkits	Encryption Tools
ISO 27000 Family of Standards	ISO 27001:2013 Assessments Without Tears Pocket Guide	Cyber Security Toolkits	

Training and Staff Awareness	Consultancy Services
• ISO 27001 Certified ISMS Foundation • ISO 27001 Certified ISMS Lead Implementer • ISO 27001 Certified ISMS Lead Auditor • ISO 27001 Internal Auditor • ISO 27005 Certified ISMS Risk Management • ISO 27001 Staff Awareness E-Learning Course • Bespoke In-House Courses and Workshops	• Business Case Development • Management and Board Briefing • Information Security Health Check • ISO 27001 Gap Analysis • ISO 27001 Certification Audit • ISO 27001 Monitoring & Review • Management System Integration
Technical Security Services	**Specialised Small Business Support Services**
• Infrastructure Penetration Tests • Web Application Penetration Tests • Wireless Network Penetration Tests • Employee Phishing Vulnerability Assessments • Software Penetration Tests • IT Health Checks • Security Audits • Architecture Reviews	• ISO 27001 Implementation Fast Track™ • Cyber Security/Information Security Health Check • Policies and Procedure Development • Live Online Support (per hour)

www.itgovernance.co.uk

IT Governance Ltd
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambs, CB7 4EA
United Kingdom

T: + 44 (0) 8450 701750
E: servicecentre@itgovernance.co.uk
W: www.itgovernance.co.uk

@ITGovernance /it-governance /ITGovernanceLtd

Protect • Comply • Thrive