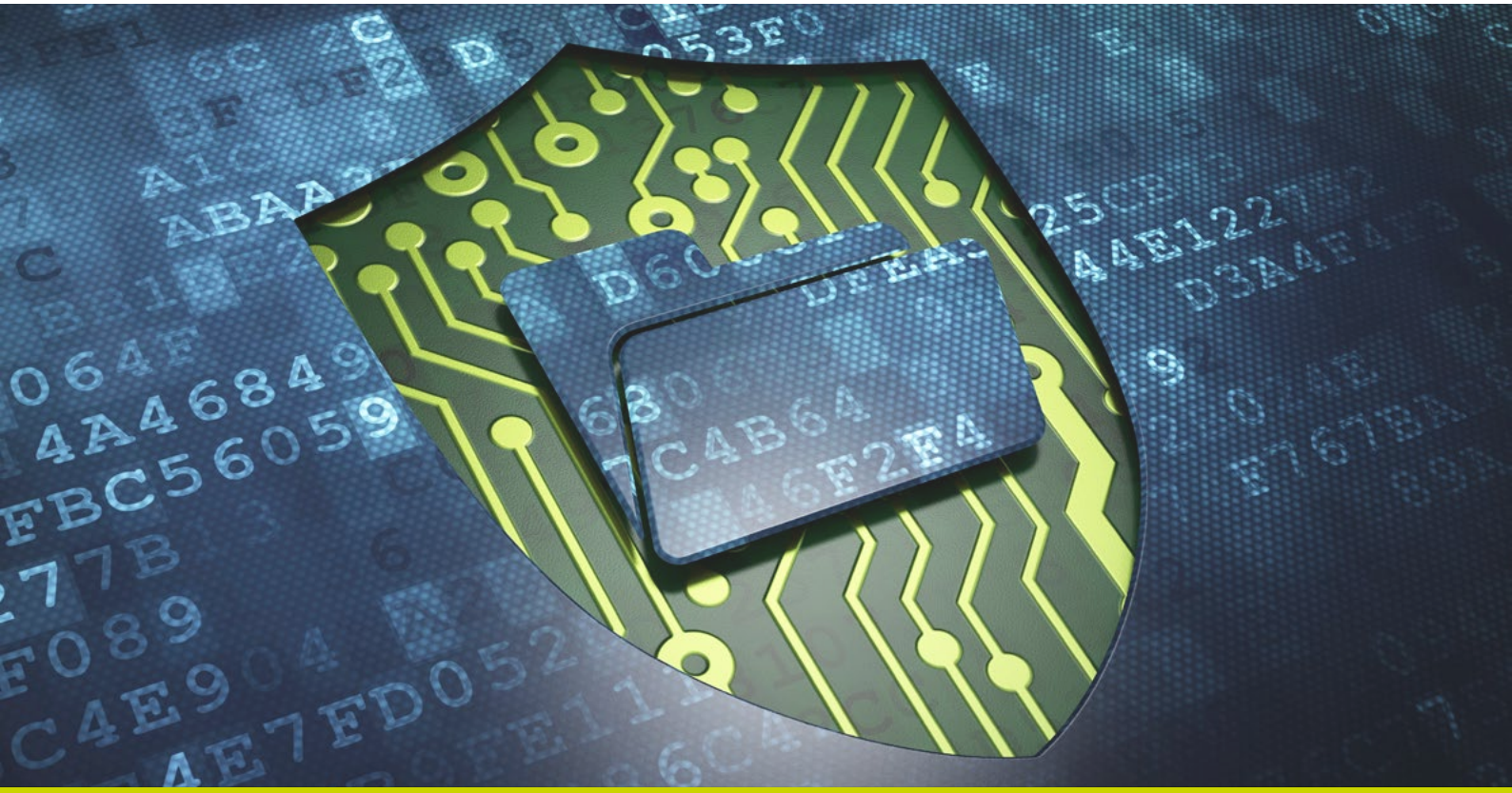
ISO 27001 Global Report
2016



"98% of respondents say that the most important benefit of ISO 27001 was improved information security, while 11% said it improved company reputation, and 8% said it improved competitiveness"

Introduction

IT Governance is proud to release the results of its second annual survey centred around the implementation challenges, benefits and experiences of ISO 27001 implementers globally.

We believe the results of this survey provide useful insights for lead implementers, auditors, consultants and heads of security teams, and will justify the continued growth and adoption of the Standard everywhere in the world.

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, the PCI DSS, ISO 27001 and cyber security solutions.

We have led ISO 27001 implementations since the inception of the Standard, helping more than 400 companies successfully achieve certification to what is often considered one of the most challenging management standards.

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

Information security and ISO 27001

ISO 27001 has become ubiquitous in information security circles globally. The Standard is now rated as the preferred choice for creating and managing a robust, dynamic and adaptable information security management system (ISMS).

The recent introduction of much tougher data protection laws, such as the EU General Data Protection Regulation (GDPR), which will be enforced on all organisations that collect or process personal data of EU residents from May 2018, will significantly increase the potential costs for organisations that are unable to demonstrate compliance. The GDPR emphasises the use of seals, marks and certification schemes to help businesses demonstrate they've taken appropriate action to implement the necessary organisational and administrative measures to protect personal data from breaches of confidentiality, integrity or availability.

ISO 27001, through its comprehensive approach to information security, presents rational and effective means of achieving demonstrable compliance with the infromation security aspects of the GDPR.

In the last ten years, the risk of cyber attacks has grown exponentially, placing cyber security risks as a top priority on board agendas. Although cyber security threats are increasing, companies are not seeing budgets rise accordingly, leading to a growing shortfall in investment. Moreover, as the global security skills shortage continues to escalate, small businesses are left vulnerable to, and often defenceless against, the onslaught of new types of assaults such as ransomware and phishing attacks.

Making ISO 27001 more accessible to small businesses has always been one of IT Governance's key objectives, through the development of innovative consultancy services, online training courses, DIY resources, manuals and guides. We believe that the results of this survey will remove misconceptions about the suitability of ISO 27001 for small companies.

Against this backdrop, we expect the demand for ISO 27001 to increase significantly over the next five years, as more organisations seek proven and effective solutions for managing their information assets, and as a more security-conscious society drives more responsible data security behaviour.

About the ISO 27001 Survey

- 53 countries participated in the survey, with a large portion of respondents representing the UK (41%), followed by India (10%) and the USA (7%).

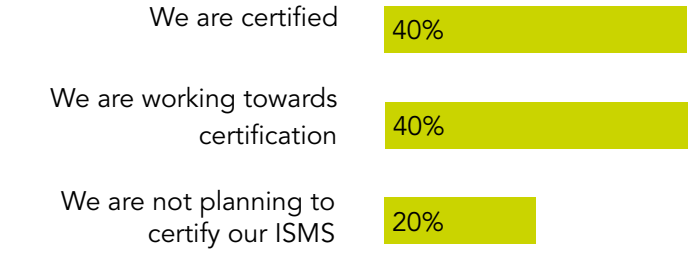
- 29% of organisations had an annual turnover of over US$100 million (£76 million), while 26% had a turnover of less than $5 million (£3.8 million).

- The majority of respondents were from the technology sector (27%), business services/ consulting (14%) and financial services (13%), followed by government/local authorities (10%).

- Individuals responsible for general IT functions (e.g. IT managers/directors) and compliance/risk managers accounted for the largest number of respondents (each accounting for 16% of respondents), followed by consultants (15%).

- 80% of respondents' organisations were either certified to ISO 27001 (40%) or were in the process of getting certified to ISO 27001 in the near future (40%).

Have you achieved ISO 27001 certification?



Alan Calder
Founder and Executive Chairman of IT Governance

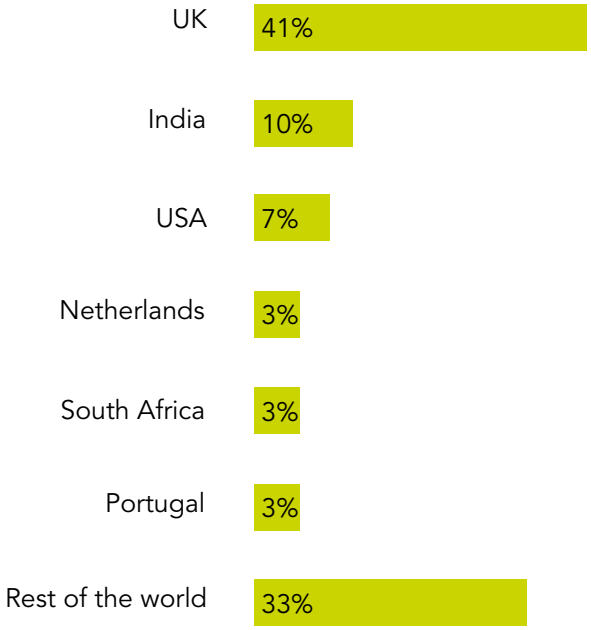
Steve Watkins
Director, IT Governance

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

They 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.

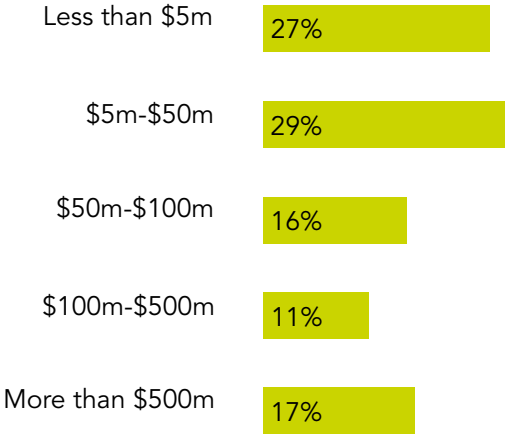
Survey participants

By country

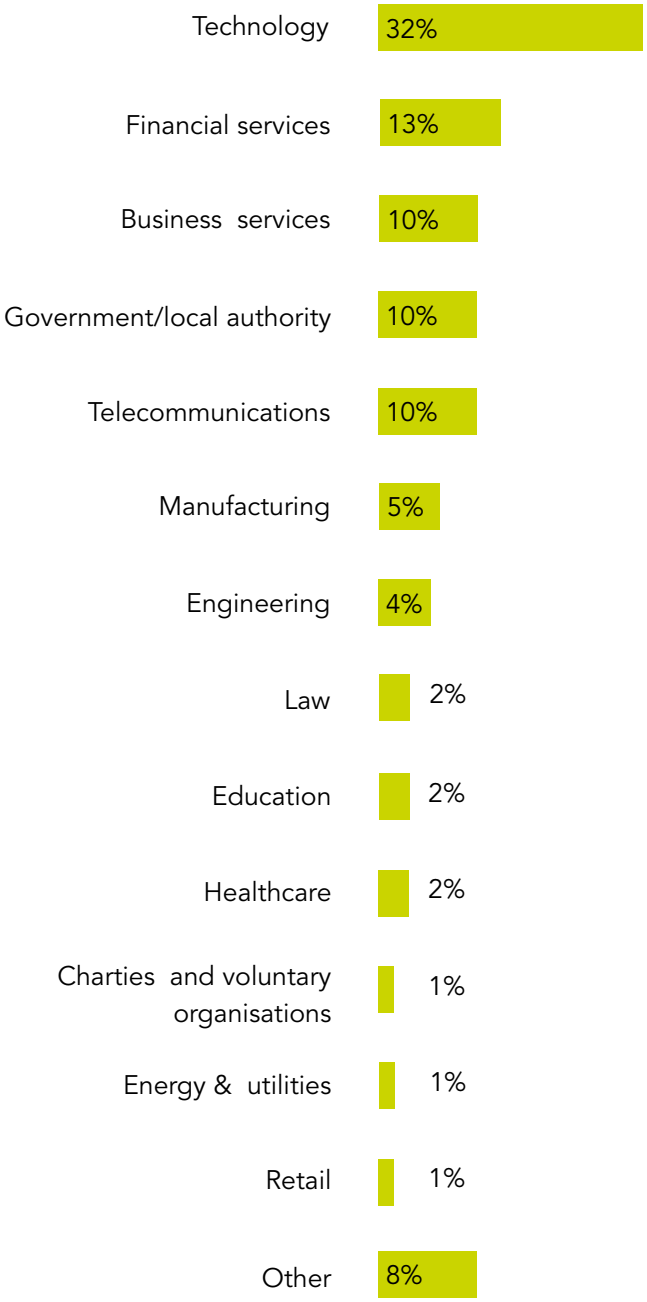


By size of organisation

By company revenue (US$)



By industry sectors



By job title

Key findings at a glance

1. ISO 27001 directly improves an organisation's information security posture

69% of respondents reported that the main driver for implementing ISO 27001 was to improve their organisation's information security posture, while 55% said that the single most important benefit of ISO 27001 has brought the organisation was improved information security.

2. Resistance from executive teams about information security is still a concern

Only 36% of respondents reported that they had no concerns about securing board buy-in for their ISO 27001 project, while 51% of respondents had problems either convincing the board about the importance of information security or securing the necessary budget and resources to implement ISO 27001.

3. Implementers struggle with key areas of ISO 27001 implementation

Obtaining employee buy-in/raising staff awareness was cited as the top challenge when implementing an ISO 27001-compliant ISMS (41%), followed by securing the right level of competence/expertise to implement the project (39%).

4. Supply chain demands are driving certification

71% of respondents received regular or occasional requests to provide evidence of ISO 27001 certification from clients or when tendering for new business.

5. The median length of time for an ISO 27001 certification project is 6 - 12 months

ISO 27001 implementation projects can be longer or shorter, depending on the organisation's size and complexity, but responses indicate that the median is 6-12 months.

6. In general, companies are not tracking implementation costs, but where costs have been tracked the average cost is less than £20,000 (US $26,000)

The majority of respondents did not keep track of their total implementation costs. For those who did, the average cost was between £5,000 (US $6,500) and £20,000 (US $26,000).

Key findings at a glance (continued)

7. Most companies do not employ a full time ISMS manager

Only 16% of companies employ a dedicated full-time ISMS manager. 19% of IT managers are responsible for the ISMS, while the CISO was responsible in 18% of cases.

8. Almost a third of respondents do not assess C, I and A separately in the risk assessment

26% reported that they did not identify the risks associated with the loss of confidentiality (C), integrity (I) and availability (A) of information separately.

9. 76% of respondents follow an asset-based risk assessment methodology

Although 76% of respondents follow an asset-based risk assessment methodology, 40% stated that they have moved/are moving to a combination of scenario/event-based and asset-based methods.

10. Only 23% use ISO 27001:2013 controls in isolation

Only 23% of respondents reported using ISO 27001:2013 controls without any additional control sets. 77% use ISO 27001:2013 controls in combination with other controls.

11. Only half of individuals managing the ISMS have a formal ISO 27001 qualification

51% of individuals managing the ISMS have a formal qualification (e.g. ISO 27001 Lead Implementor/Lead Auditor).

12. There is a strong need for external assistance and support

54% of respondents use external providers of penetration testing providers, while 51% rely on external consultants to help them implement the ISMS.

13. ISO 27001 delivers ROI

52% of companies felt that the cost of achieving ISO 27001 certification was fully justified by the benefits it delivers, while 21% felt it was in line with other management system standard implementations.

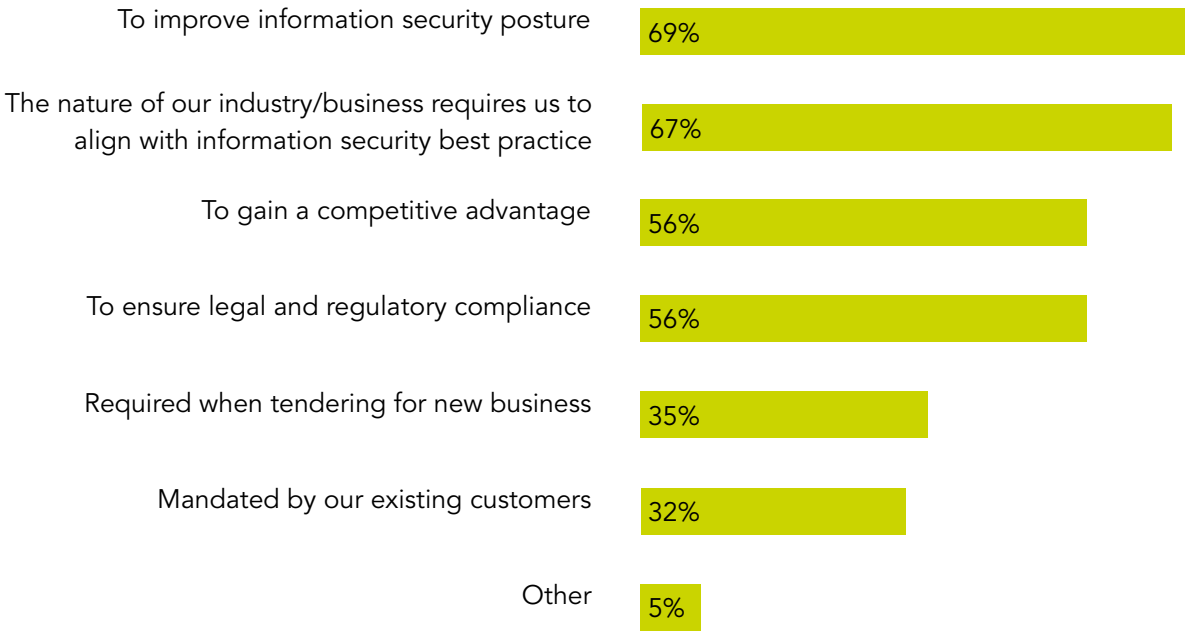
Finding 1

ISO 27001 delivers direct benefits for improving an organisation's information security posture

69% of respondents reported that the main driver for implementing ISO 27001 was to improve the organisation's information security posture. In addition, 55% of companies said that the single most important benefit of implementing ISO 27001 was improved information security across the whole organisation.

Implementing and maintaining an ISO 27001-compliant information security management system (ISMS) presents a systematic approach to managing the security of sensitive information. An ISMS is designed to identify, manage and reduce the range of threats to an organisation's information and information-related assets are regularly subjected.

What are the main driver/s for implementing ISO 27001 in your organisation?

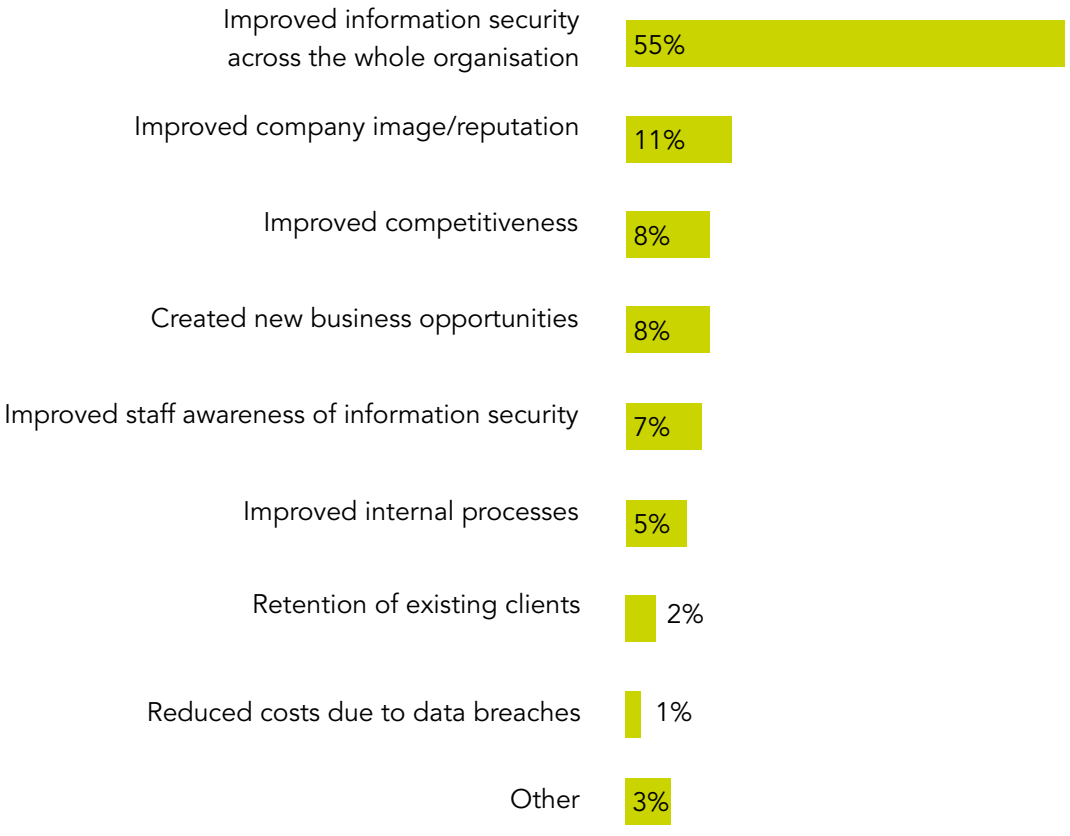


Finding 1 (continued)

The continued escalation of cyber attacks, combined with an increasingly regulated data security landscape, means many companies are coming to realise the benefits of implementing ISO 27001. It is no surprise that, in terms of uptake, ISO/IEC 27001:2013 is now among the fastest-growing management system standards in the world.

In addition to improved information security, 56% of respondents said that the main driver for implementing ISO 27001 was to achieve a competitive advantage. ISO 27001 certification is growing in demand as a contractual requirement for suppliers bidding for new business and demonstrates credibility when tendering for contracts. It has been proven that conformity to the Standard can make the difference between winning and losing tenders.

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



Finding 2

Resistance from executive teams about information security is still a concern

Only 36% of respondents reported that they had no concerns about securing board buy-in for the ISO 27001 project, and said that the board was supportive right from the start.

A further 51% of respondents had problems convincing the board about the importance of information security, or securing the necessary budget and resources to implement ISO 27001.

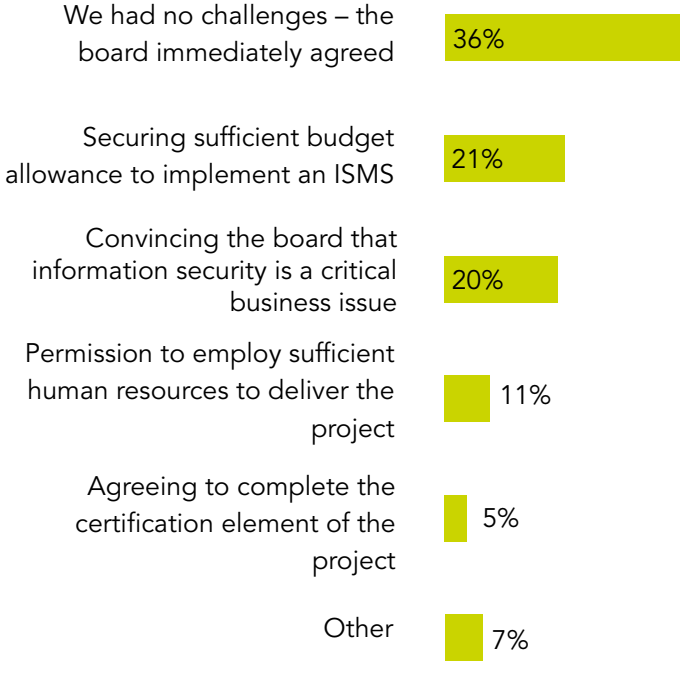
A critical ingredient for the successful implementation of ISO 27001 is top management commitment, the absence of which will make it nearly impossible to establish, implement and maintain an effective ISMS.

A plausible explanation for some boards backing the project from the start could be that they were already aware of and understood the benefits that ISO 27001 offers. It is incumbent upon the executive team to take ownership of information security risks, and to be informed about how the organisation will defend itself against and respond to such risks.

Based on the above, it is clear that information security teams often struggle to make a convincing business case for an ISO 27001 ISMS implementation project.

A detailed ISO 27001 gap analysis is often the starting point for a more complex ISO 27001 project, and enables teams to justify the benefits of implementing an ISMS by providing useful data for building a solid business case. Such a business case should weigh up the benefits against the potential losses of confidentiality, availability and integrity of data, in addition to the reputational and financial damage associated with a data breach.

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



Finding 3

Implementers struggle with key areas of ISO 27001 implementation

41% of respondents cited obtaining employee buy-in and raising staff awareness as the top challenge when implementing ISO 27001. Poor staff awareness is a common theme in information security circles, and numerous surveys continue to highlight the dangers of poor information security awareness among staff.

Be it accidental or malicious, the exposure of data because of staff negligence is responsible for a high rate of data loss, so it is essential for organisations to implement effective measures to overcome staff ignorance of security risks.

Resource shortage is another common thread that runs across all organisations, irrespective of country or industry: 39% of respondents said they battled to obtain the right level of competence and expertise to implement the project.

Competition for appropriately qualified staff is stiff, and salaries continue to rise in the battle to attract suitably skilled candidates. These salaries are often beyond levels that smaller organisations can afford.

As a result, companies either choose to outsource their ISMS implementation project to qualified consultants, or appoint internal teams that can manage the project themselves. Whether or not these teams have the necessary expertise is addressed later in this report.

Other notable challenges experienced by respondents were being able to properly interpret the Standard's requirements (31%), and creating and managing the ISMS documentation (28%). Implementing and maintaining an ISMS requires up-to-date, accurate and compliant documentation, and requires a lot of work to get it right.

Alan Calder, the founder and executive chairman of IT Governance, says: "The key test of the ISMS documentation is that it should be adequate, but not excessive, and that it enables each of the processes to be systematically communicated, understood, executed and effective so as to be repeatable and dependable."

In addition to the above, other notable challenges include reporting on and maintaining the ISMS (24%), and conducting the risk assessment (22%).

Without adequate reporting and monitoring, the process of continually improving the ISMS will not be effective. Continual improvement is one of the cornerstones of ISO 27001 that sets it apart from many other information security programmes.

Finding 3 (continued)

At the centre of any mature ISMS should be a comprehensive, well-planned and well-executed information security risk assessment that is designed to identify the relevant assets or risks, and enable the business to prioritise the different security measures and controls. Although ISO 27005 provides guidelines for conducting a risk assessment, the process is not always clear for newcomers to the Standard, not least because the current version of ISO 27005 (2011) is still aligned to the less flexible 2005 version of ISO 27001.

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

Finding 4

Supply chain demands are driving certification

71% of respondents received either regular or occasional requests to provide evidence of ISO 27001 certification from clients or when tendering for new business. 37% of respondents receive regular requests.

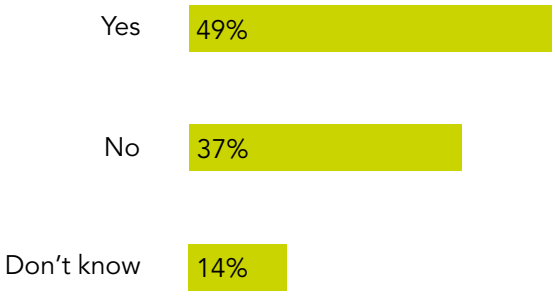
By providing a globally accepted indication of security effectiveness, ISO 27001 certification significantly reduces the need for repeated client audits, reducing the number of external audit days, and presents significant savings in terms of preparatory work when entering into contracts.

Likewise, ISO 27001 flows down the supply chain: 49% of respondents say they requested evidence of ISO 27001 certification from their suppliers in the last 12 months.

Suppliers are often an attractive target for hackers as they can provide an easy way into larger organisations. 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 5

The median length of time of an ISO 27001 certification project is 6 - 12 months

The median response given was 6-12 months, which was in common with 51% of respondents. This is in line with last year's report results of 47%.

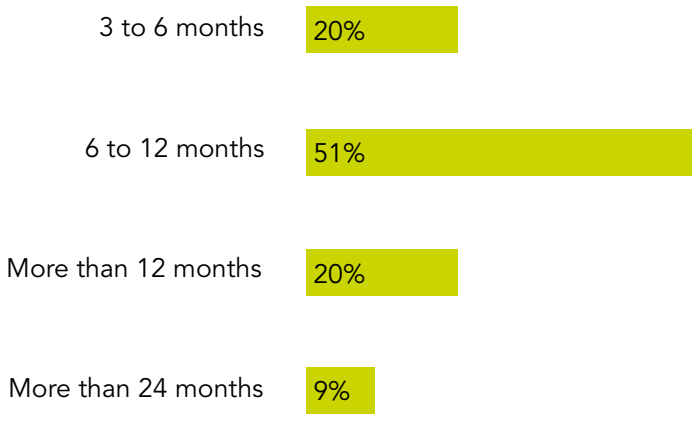
20% said it took between 3 and 6 months to achieve certification (in 2015, this figure was 29%), while 20% said it took more than 12 months (19% in 2015). 8.5% took more than 2 years to complete their certification project (5% in 2015).

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. Small companies with a single office location and few staff may be able to achieve certification in less than three months if they rely on external help.

Larger organisations, typically with more complex scopes, will take longer, but this will also depend on their internal structure, existing practices, project plan and resource schedule. 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.

Mobilising internal experts and calling in external help can considerably accelerate a project, especially if there is a tight deadline. Organisations wishing to achieve certification to ISO 27001 ISMS within a short period of time or agreed timeline can opt for FastTrack consultancy services.

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



Finding 6

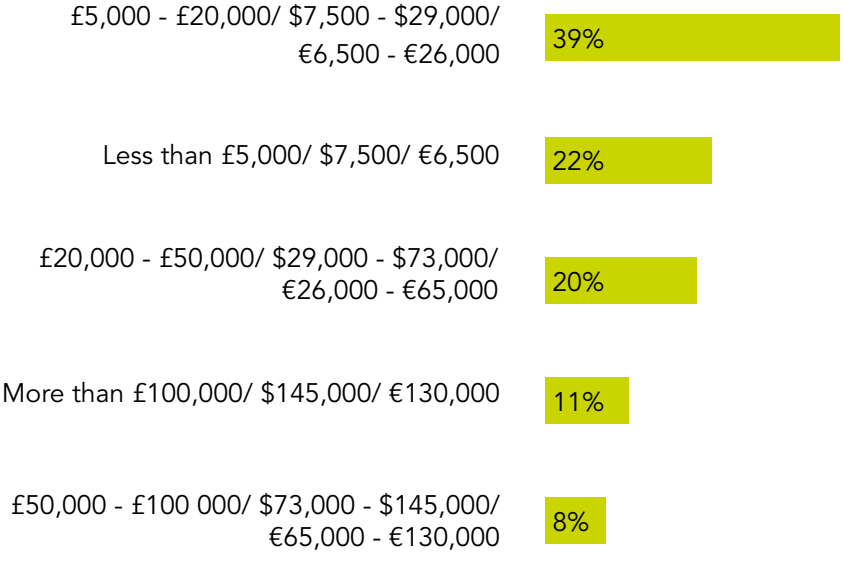
Where implementation costs have been tracked, the average cost is less than £20,000

The majority of respondents who have implemented or are in the process of implementing ISO 27001 (62%) did not track their total implementation costs. Of the respondents who did, the average cost of implementing an ISO 27001-compliant ISMS, excluding certification fees, was between £5,000 (US$6,500) and £20,000 (US$26,000) (39%).

Given that resistance to information security from executive teams is still a concern (Finding 2), it is essential that security teams are capable of articulating the value of their information security programmes when attempting to justify the security budget.

82% of small businesses with turnovers of less than £3.8 million/US$5 million (who had tracked their implementation costs), reported that the implementation of an ISO 27001-compliant ISMS cost less than £20,000 (US$26,000). For 50%, it cost less than £5,000 (US$6,500). This indicates that ISO 27001 is totally within reach for small businesses, contrary to what is commonly believed, especially when implemented in an intelligent manner.

If you have quantified it, what was the cost to your organisation of implementing an ISO 27001-compliant ISMS in the first year of certification, excluding certification fees?



** Currency exchange rates at the time of the survey*

Finding 7

Most companies do not employ a full time ISMS manager

Only 16% of companies employ a dedicated full-time ISMS manager. IT managers were responsible for the ISMS in 19% of case, while the CISO was responsible in 18% of cases.

It is interesting to note that there was no major difference between small and large organisations in terms of the perceived benefits of employing a full-time ISMS manager, despite the fact that large organisations may be more in need of a full-time resource to manage the ISMS.

In companies with annual turnovers of more than US$100 million, 21% employed a full-time ISMS manager, while the CISO was responsible for the ISMS in 31% of cases. In companies with less than a $5 million turnover, a full-time ISMS manager was employed in 13% of cases, while the IT manager took on the role in 23%.

The ISMS manager has a prominent role to play in organisations that are certified or considering certification to ISO 27001. Not only must the individual be technically experienced, but they should be able to work across all areas of the business in order to understand and apply suitable solutions for the range of challenges. Such a position will usually hold responsibility for developing, implementing and maintaining the ISMS, and providing information security strategy, policy, risk advice and guidance to assist in the delivery of business objectives.

Who manages the ISMS in your organisation?

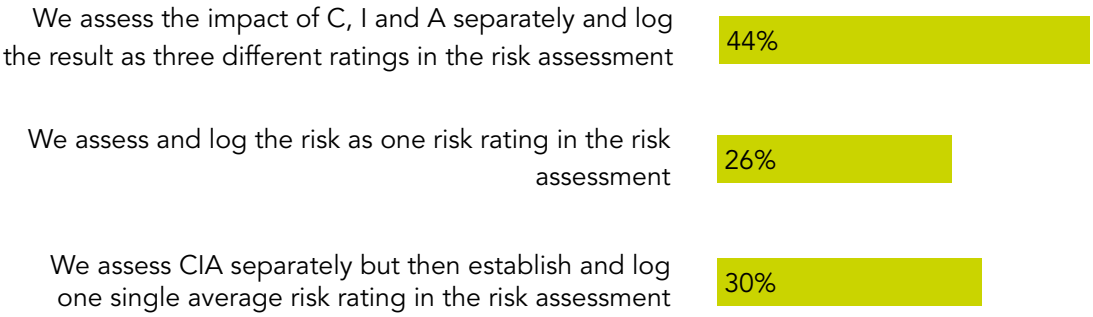
Finding 8

Almost a third of respondents do not assess C, I and A separately in the risk assessment

Although 74% of respondents reported that they conduct risk assessments by identifying risks associated with the loss of confidentiality (C), integrity (I) and availability (A) of information separately, 26% reported that they assessed the C, I and A as one rating.

The increased flexibility in the information security risk assessment requirements in the 2013 version of the Standard, increases the extent to which it can easily be applied to small and micro organisations.

Does your risk assessment consider identifying the risks associated with the loss of confidentiality (C), integrity (I) and availability (A) for information as three separate measures, or do you use one measure to establish your risk rating?



Finding 9

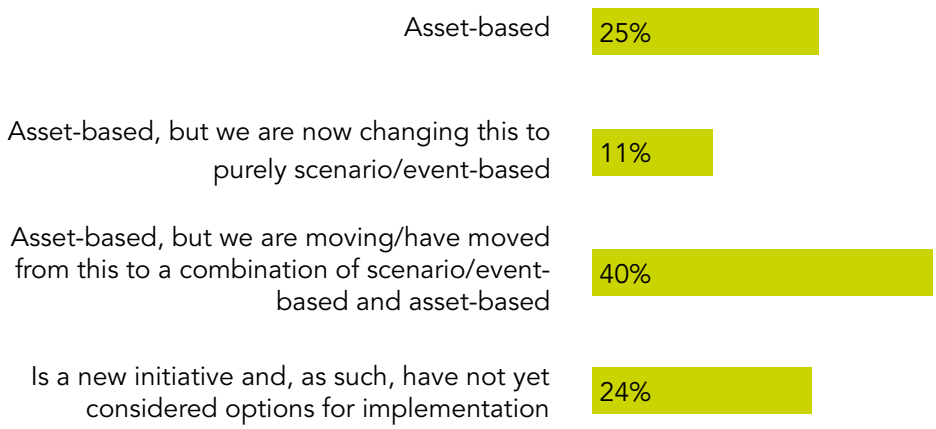
76% of respondents follow an asset-based risk assessment methodology

Although 76% of respondents follow an asset-based risk assessment methodology, 40% stated that they have moved/are moving to a combination of scenario/event-based and asset-based methods.

When ISO/IEC 27001:2013 was introduced, it provided more flexibility with regard to the information security risk assessment methodology an organisation can adopt. More companies are moving towards a blended approach that allows additional measures to identify risks as events, rather than purely as the result of threat-vulnerability combinations for information assets.

An asset-based information security risk assessment methodology is still considered by information security experts to be the most robust and effective way of identifying the range of risks that can influence an organisation's information security posture.

Your ISO 27001:2013-aligned risk assessment methodology is best described as:



Finding 10

Only 23% use ISO 27001:2013 controls in isolation

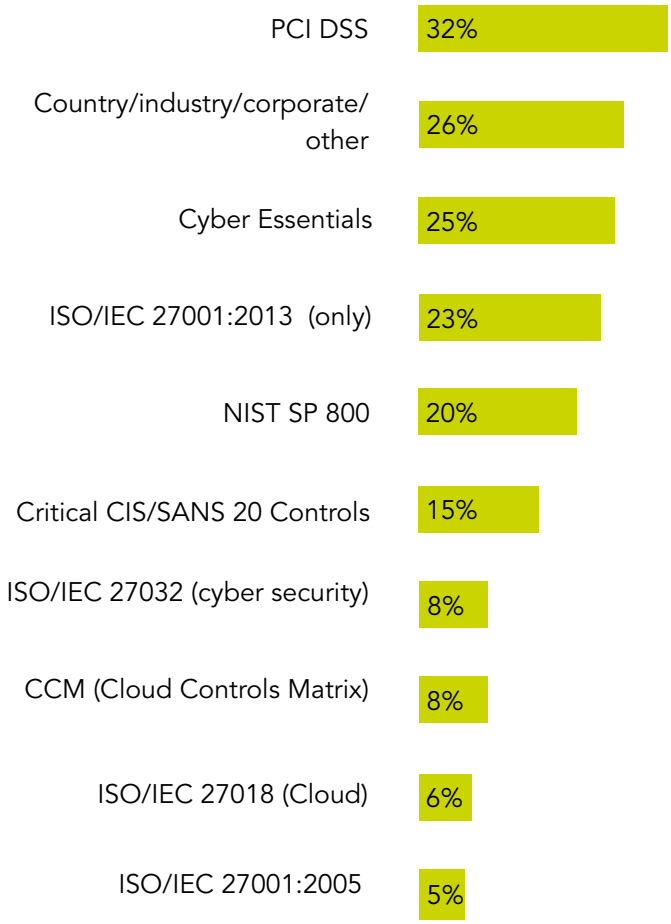
The most popular control sets used in addition to ISO 27001:2013 were the PCI DSS (32%), followed by Cyber Essentials (25%) and NIST SP 800 (20%). The popularity of Cyber Essentials can be attributed to the fact that a high volume of respondents were from the UK (41%).

26% of respondents also reported using country/industry-specific or other corporate controls.

5% of respondents were also still using the controls sourced from ISO 27001:2005, mapping them onto the 2013 Annex A control set.

Only 23% of respondents reported using ISO 27001:2013 controls without any additional control sets. 77% use ISO 27001:2013 controls in combination with other controls.

Which of the following additional cyber security/general controls, other than those provided by Annex A, are you using in your ISMS (if any)?



Finding 11

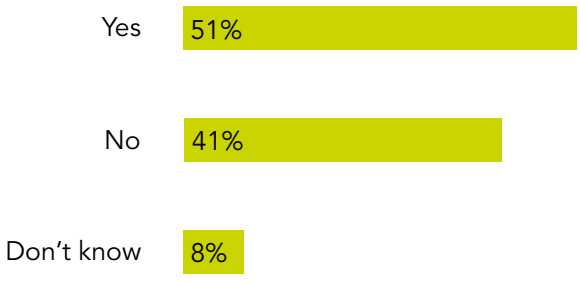
Only half of individuals managing the ISMS have a formal ISO 27001 qualification

51% of individuals managing the ISMS have a formal ISO 27001 qualification (for instance an ISO 27001 Lead Implementer or Lead Auditor qualification). More than one third of the respondents (35%) who admitted that the ISMS manager did not have any formal training were considering additional training, although 40% said they didn't have control over the training decision.

Considering the numerous challenges that organisations are experiencing with implementing the ISMS (based on Finding 3), organisations should be prioritising training for their information security/ISMS teams to ensure that they are equipped with the right tools and knowledge in relation to the processes to follow to ensure the optimal performance of the ISMS.

With the growth of ISO 27001's popularity over the past decade, there is an increasing need for professionals with ISO 27001 qualifications to fulfil information security roles.

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



Finding 12

There is a strong need for external assistance and support

The survey results show that organisations rely on external advice and technical expertise to assist them with the management of their ISMS. 54% of respondents use external penetration testing providers, while 51% rely on external consultants to help them implement their ISMS. 39% outsource their e-learning staff awareness programmes, and 32% use documentation toolkits.

The above point underlines the increased need for upskilling and empowering ISMS managers to be able to fulfil key ISMS management duties within the organisation.

Are you using any of the following externally developed or delivered support tools or consultancy assistance to help you achieve/maintain certification?

Finding 13

ISO 27001 delivers ROI

52% of respondents who had already implemented ISO 27001 or were in the process of implementing the Standard felt that the cost of achieving certification to ISO 27001 was fully justified by the benefits it delivers. 21% believed it was in line with other management standard system implementation projects.

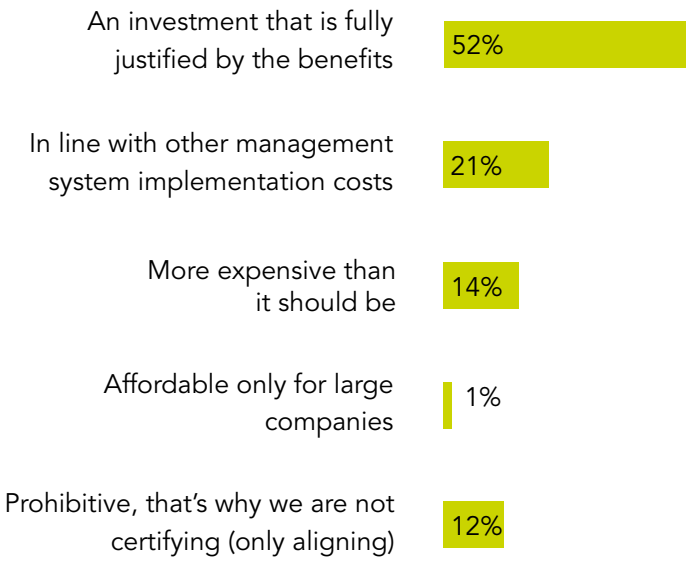
Given the fact that only 45% of respondents have tracked their implementation costs, it is reassuring to see that only 15% felt that the certification costs were too high. This could indicate that ISO 27001 delivers a sufficient, visible return without needing a detailed cost-benefit analysis.

Implementing an ISO 27001-compliant ISMS delivers lesser-known intangible benefits as well as the obvious ones. These include an improvement in company culture because of the Standard's holistic approach of covering the whole organisation and encompassing people, processes and technology. This enables employees to readily understand risks and embrace security controls as part of their everyday working practices.

In addition, ISO 27001 also improves structure and focus. When a business grows rapidly, it doesn't take long before there is confusion about who is responsible for which information assets. The Standard helps businesses become more productive by clearly setting out information risk responsibilities.

Despite this, 12% of respondents felt that certifying to ISO 27001 was affordable only for large companies.

Would you characterise certifying to ISO 27001 as:



Protect • Comply • Thrive

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

ISO 27001 packaged consultancy

What is included?	ISO 27001 The Basics	ISO 27001 Do It Yourself	ISO 27001 Get A Little Help	ISO 27001 Get A Lot Of Help
ISO 27001:2013 (standard PDF)	✓	✓	✓	✓
ISO 27002:2013 (standard PDF)	✓	✓	✓	✓
ISO 27000:2016 (standard PDF)	✓	✓	✓	✓
Nine Steps to Success (eBook)	✓	✓	✓	✓
IT Governance: An International Guide to Data Security (eBook)	✓	✓	✓	✓
ISMS Standalone Documentation Toolkit		✓	✓	✓
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.

Contact us today on servicecentre@itgovernance.co.uk or call +44 (0)845 070 1750.

Management standards	Books and guides	Documentation toolkits
• ISO 27001:2013 • ISO 27002:2013 • ISO 27032:2012 • ISO 27005:2011 • ISO 27000 family of standards	• Nine Steps to Success • The Case for ISO 27001 • An Introduction to Information Security & ISO 27001 • IT Governance - An International Guide to Data Security and ISO27001/ ISO27002, Sixth Edition	• ISO 27001:2013 toolkits and toolkit bundles
Software	**Technical and qualifications**	**Software awareness**
• Information security risk assessment software vsRisk™ Standalone • Information security risk assessment software vsRisk™ Multi-user • UK IT Legal Compliance Database	• 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 • Information Security and ISO 27001 Staff Awareness e-learning course • Phishing Staff Awareness e-learning course
Bespoke consultancy	**Packaged consultancy**	**Technical testing**
• Business Case Development • Management and Board Briefing • Information Security Health Check • ISO 27001 Gap Analysis • ISO 27001 Monitoring & Review • Management System Integration	• ISO 27001 FastTrack™ and FastTrack™ Online • ISO 27001 Internal Audit • ISO 27001 ISMS Managed Service • ISO 27001 Get A Lot Of Help	• Infrastructure Penetration Tests • Web Application Penetration Tests • Wireless Network Penetration Tests • IT Health Checks • Security Audits • Architecture Reviews • Simulated Phishing Attack

Protect • Comply • Thrive

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