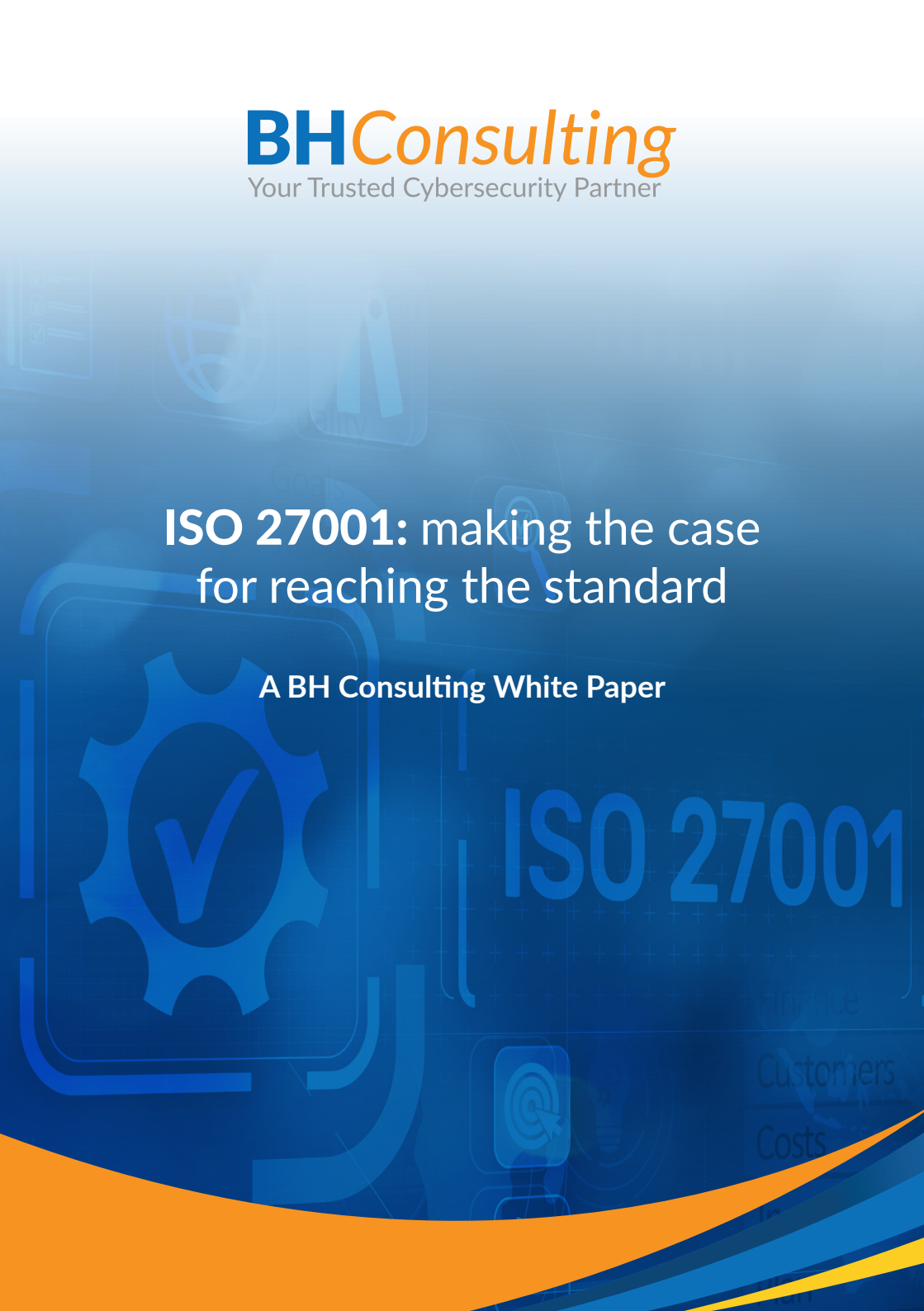
BH Consulting
Your Trusted Cybersecurity Partner

ISO 27001: making the case for reaching the standard

A BH Consulting White Paper



About this guide

Good information security, it's often said, is a combination of people, process, and technology. The ISO 27001 information security standard focuses strongly on the process, which in turn helps to guide the optimal allocation of people and technology resources. Simply put, it is a systematic, repeatable way of following best practice for protecting and securing critical information.

Information security is not just about compliance, demonstrating best practice or implementing the latest technical solutions. It is about managing the risks posed to the business by the accidental or deliberate misuse of confidential information. It is important to note that no matter what industry, the private or public sector, every organisation has confidential information it needs to protect.

Using a standard like ISO 27001 is a helpful framework for applying security effectively, at a time when the need for it is clearer than ever. Cybercrime threats are increasing all the time in volume and nature, carrying the risk of disruption to business operations, not to mention the financial cost. At the same time, growing numbers of organisations must comply with industry-specific regulations or national laws that require them to take proactive measures to protect confidential information and prevent or respond to security incidents and breaches.

ISO 27001 is well established, having been around for more than 15 years. It is internationally recognised, and both vendor- and technology-neutral. It takes a risk-based approach to securing information, which makes it suitable for organisations of all sizes, from fewer than 10 people to ones with thousands of employees and contractors.

This white paper provides an overview of the business benefits of the standard, and how it can help organisations of all sizes to address their ongoing information security needs.

Background

As a result of increasing regulatory and industry compliance requirements, information security is becoming a board-level item. Even for companies not impacted by industry-specific regulations such as the US Sarbanes-Oxley Act or the Basel II accord, there are other requirements such as the General Data Protection Regulation they need to follow. Companies are now faced with the dilemma of ensuring their information is secure enough to be compliant. However, therein lies the rub. How secure is secure enough? Does being compliant mean that your information and systems are secure? Indeed, does being secure mean that you are compliant?

The problem many companies face is that there are no recommended benchmarks or minimum grades clearly stated in any of these compliance regulations. Those responsible for securing a company's information face the onerous task of trying to determine how best to implement effective security controls to not only ensure compliance, but also secure their systems and information.

The ISO 27001 Information Security Standard offers companies a way to address this problem. By adopting the risk and standards-based approach to implementing an Information Security Management System in accordance with ISO 27001, companies can reap many advantages, not least being better able to demonstrate compliance with legal and industry regulatory requirements.

It is important to note that ISO 27001 can simply be used as a framework against which a company can implement and measure its Information Security Management System (ISMS) against, without necessarily having to be accredited. This is particularly useful for companies wishing to ensure they are implementing an effective ISMS but may not want the expense and overhead of being audited.

For those that do choose to follow the audit route, ISO 27001 accreditation gives independent third-party verification that their ISMS meets an internationally recognised standard. This provides the organisation, and its customers and partners, with the confidence that it manages its security in accordance with recognised and audited best practice.

What is ISO 27001?

ISO 27001, also known as IEC 27001:2013, is an internationally recognised standard of good practice for information security. It takes a risk-based approach to securing an organisation's most valuable information – whether that's in digital or physical form.

The standard has no ties to any specific vendor or technology. Rather than focusing on the latest technical solutions, ISO 27001 helps organisations to manage risks to the business from accidental or deliberate misuse of confidential information. ISO 27001 enables a company to implement a qualitative approach to risk management, and gives mechanisms to address, reduce and manage those risks.

In effect, ISO 27001 provides a framework for best practice in managing information security. Unlike self-regulated standards, being certified to ISO 27001 – for those that choose to do so – involves having an independent external organisation verifying at least once a year that you operate your security appropriately.

Who needs ISO 27001?

Every organisation, regardless of industry, has confidential information: that could be customer details, payroll information or credit card numbers, business plans, financial information or intellectual property. Whether regulated or not, organisations have a duty to protect that information.

The latest version of the ISO 27001 standard provides a set of standardised requirements for an information security management system (ISMS) for short. This combines into one place the various processes, documents, technology and people that you will use to manage, monitor, audit and improve your information security. Becoming certified to the standard provides a process-based approach for setting up, operating, monitoring and maintaining an ISMS.

Let's address a misconception: using a standard like ISO 27001 has nothing to do with how large an organisation is. It's better to think of ISO 27001 in terms of how important you consider your organisation's or your customers' data. That could be business plans, financial information, intellectual property, payroll details, or credit card numbers.

Business benefits of ISO 27001

The ISO 27001 Information Security Standard gives confidence and reassurance that your security programme is operating optimally. Following the ISO 27001 framework, or becoming certified to the standard, shows customers, partners and other key stakeholders that you value their information and your organisation's reputation – and that you are doing so according to recognised and audited best practice.

One challenge facing companies when implementing an Information Security Management System is quantifying the benefits the company can derive from it. It's possible to demonstrate tangible results from investing in new hardware or in staff, it can be quite difficult to demonstrate to senior management the benefits from investing time, resources and money in an ISMS. Here are some business-focused benefits:

- *Increased reliability and security of systems*

  Security is often defined as protecting the Confidentiality, Integrity and Availability (CIA) of an asset. Using a standards-based approach, which ensures that adequate controls, processes and procedures are in place will ensure that the above goals are met. Meeting the CIA goals of security will also by default improve the reliability, availability and stability of systems.

- *Increased profits*

  Having stable, secure and reliable systems minimises the potential for interruption – thereby increasing their availability and productivity. In addition, using a standards-based approach to information security demonstrates to customers that the company can be trusted with their business. This can increase profitability by retaining existing customers and attracting new ones.

- *Reduced costs*

  A standards-based approach to information security ensures that all controls are measured and managed in a structured manner. This ensures that processes and procedures are more streamlined and effective thus reducing costs. Some companies have found they can better manage the tools they have in place by consolidating redundant systems or re-assigning other systems from assets with low risk to those with higher risk.

- *Easier regulatory compliance*

  Having a structured Information Security Management System in place makes the task of compliance much easier. Growing numbers of companies and public bodies are considering ISO 27001 to support compliance with GDPR. Similarly, ISO 27001 is useful for managing compliance with security frameworks such as the EU NIS directive, or HIPAA.

- *Improved management*

  Knowing what is in place and how it should be managed and secured makes it easier to manage information resources within a company. Becoming certified has been shown to help smooth the due diligence process during an acquisition. It may also reduce an organisation's cyber insurance premiums. By definition, any organisation that has undergone the certification process can prove it operates a robust risk assessment process.

- *Improved customer and partner relationships*

  By demonstrating the company takes information security seriously, customers and trading partners can deal with the company confidently knowing that the company has taken an independently verifiable approach to information security risk management. Third-party risk is a legitimate concern for large businesses – think of how attackers breached Target's network through a supplier. The larger the customer, the more rigorous their supplier due diligence tends to be. Often, companies must show they follow best practice information security to become an approved supplier to a larger enterprise. Security questionnaires now feature regularly in many tendering processes, and some specifically ask for security certification or attestation.

Successful certification: do's and don'ts

It is worth repeating the point: ISO 27001 applies to all types of information. Consequently, it affects the entire business, not just the IT department. Although IT or information security professionals will probably be the ones initially making the case for certification, but experience shows that the most effective way to get management buy-in is to translate information security into business language.

In many ways, it's a classic 'chicken-and-egg' scenario: without full support from management, successful ISO 27001 implementation is unlikely. Yet a successful implementation ensures you have full support.

With a solid business case for getting certification, how do you ensure the process itself is a success? In this section and the following one, here are some high-level tips for making that process run smoothly and successfully:

1. Do it for the right reasons: to assure customers, stakeholders or external overseer that you keep data secure.

2. Do obtain full support from senior management. Ensure they're bought into the programme and that they provide the right resources and budget to ensure success.

3. Do get buy-in from all parts of the business. ISO 27001 is an information security standard, not an IT standard.

4. Do ensure information security is a regular agenda item on senior management meetings, not just an annual review. Have management actively review and sign off on security policies and attend security awareness training.

5. Don't chase certification purely to satisfy a sales requirement or for marketing purposes. Otherwise you don't get the correct level of focus on the standard. Treating it as a box-ticking exercise makes it difficult to achieve and maintain certification.

Six steps to becoming certified

At BH Consulting, we recommend starting the certification process by gaining support from the highest levels within the business. This is critical to ensuring not just a successful project but a sustained culture of security in the organisation, regardless of its size. Whether your organisation wants to measure its current information security practices against ISO 27001, or achieve certification to the standard, we provide the following six steps:

1 Gap analysis

This phase determines the current status of your ISMS against the requirements of ISO 27001. Through first-person interviews, we evaluate the security controls and identify areas for improvement to enable certification to the standard. At the end of this phase, we produce a report outlining areas to address and steps to doing so.

2 Risk assessment workshops

The workshop entails identifying information security assets, developing a risk assessment methodology that suits the organisation's needs, identifying risks and building a risk treatment plan. This is another critical stage in the process, because it determines what levels of risk the organisation is prepared to accept, and it identifies unacceptable risks. This process also involves identifying human, process or technical controls to manage the risks appropriately. The outcome of this stage is a comprehensive document along with tools to enable the business to maintain its risk management and risk assessment programmes.

3 Aligning your ISMS with ISO 27001

We can help with aligning your ISMS with the standard. We conduct a thorough exercise that encompasses: clauses of the standard that are relevant to your ISMS; an overview of the organisation's activities and services; current information security manuals or policies; business continuity strategy; copies of internal audits to date; control of documents within the scope of the ISMS; how the organisation can identify any weaknesses within its ISMS; outlining how internal ISMS audits will be conducted, by whom and how often; describing the risk assessment methodology; a copy of the information security risk assessment report, that includes identified unacceptable risks, as well as risk treatment plans to mitigate those risks.

4 *Implementation*

To achieve certification to ISO 27001, it is essential to show that you are applying the standard rigorously to your ISMS. This means ensuring all policies and procedures are properly documented an up to date; making all staff aware of the relevant processes and procedures; assigning certain staff with information security roles and making clear what those roles entail; maintaining audit logs and other evidence as proof you adhere to policies and procedures.

5 *Internal audits*

An internal audit that regularly checks the ISMS, or sections of it, is a requirement for continuous certification to ISO 27001. This ensures it continues to follow the guidelines se out in the standard. We can provide this audit as a service, with scheduled audits to an agreed timeframe with your organisation.

6 *Training*

We provide a range of training courses around ISO 27001 that outline the principles of information security and their importance to an organisation. We combine course materials with practical exercises, tips and case studies. The training helps information security managers, senior managers, quality professionals and IT staff to identify the benefits of implementing ISO 27001 and to understand the basics of information risk management.

ISO 27001 extends privacy controls : ISO 27701

The International Organization for Standardization (ISO) recently published an extension to ISO/IEC 27001 and 27002 for privacy information management. At BH Consulting, we believe that complying with the standard has many business benefits which we have outlined in this white paper. What's more, the process and rigour that the standard applies to information security means it's very useful as a way to manage compliance with the General Data Protection Regulation (GDPR). For example, one of the requirements under the regulation is to report breaches within 72 hours of discovering one. The ISO 27001 framework is very useful for helping organisations to develop a solid incident response plan that covers the three pillars of IT, people and processes.

When the ISO announced the ISO 27701 extension, it said it specifies requirements "for establishing, implementing, maintaining and continually improving a privacy-specific information security management system. In other words, a management system for protecting personal data (PIMS)."

It builds on the ISMS that ISO 27001 requires all certified organisations to put in place. To recap, an ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes. The ISO 27701 extension "provides the necessary extra requirements when it comes to privacy", the ISO said. Dr Andreas Wolf, chair of the technical committee that developed the standard, said that almost every organisations handles personally identifiable information, and that protecting it "is not only a legal right but a societal need".

He added: "ISO/IEC 27701 defines processes and provides guidance for protecting PII on an ongoing, ever evolving basis. Because being a management system, it defines processes for continuous improvement on data protection, particularly important in a world where technology doesn't stand still."

It is important to clarify that the new addition of 27701 is not a standard by itself but an extension to the existing information security standard. This means organisations cannot get certified to it directly. You must first become certified to ISO 27001 and then to this standard. It is worth noting that ISO 27701 is a privacy standard and is designed to encompass privacy laws and regulations around the world. While not specific to GDPR, it can be used for it. In summary, it is a privacy standard designed to enable organisations to meet any and/or all of their privacy obligations including, but not exclusive to GDPR.

Conclusion

While not guaranteeing 100% security, no standard or system can, ISO 27001 allows a company to implement a qualitative approach to risk management whilst providing mechanisms to address, reduce and manage those risks. Companies serious about information security should take a long hard look at ISO 27001. It could help answer the question "how secure is secure enough?"

Disclaimer:

BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

For more information please contact us:

+353 (0)1 440 4065

info@bhconsulting.ie

www.bhconsulting.ie