SYNERGOS CONSULTANCY LTD

ISO 27001

Putting the safety and security of your business information first.

ISO 27001

ISO 27001 explained

This guide is designed to introduce you to the ISO 27001 Information Security Management System, including outlining the purpose of it, the benefits of obtaining certification, and the steps involved in achieving and maintaining it — it's easier than you might think!

What is ISO 27001?

ISO frameworks are a set of internationally recognised guides and processes for organisations to use.

ISO 27001, developed by the International Standards Organisation (ISO) in partnership with the International Electrotechnical Commission (IEC), provides a framework for a business or organisation of any size to protect its information through an Information Security Management System (ISMS). The latest review was in 2013, so it is often denoted as ISO 27001:2013.

The ISMS facilitates the improvement in protection for data and for the physical environments, securing assets such as financial information, intellectual property, employee details, or information held by third parties. It takes into account the processes that a business currently has in place, and provides a holistic, risk-based approach to drive continuous improvement.

ISO 27001 certification demonstrates a business' commitment to the security and proper management of its information and data — something that many stakeholders and customers require as standard.

What is **required?**

The purpose of ISO 27001 is to protect the confidentiality, integrity and availability of a business' data. To do this, an organisation must identify information security risks and then put systems in place to mitigate or reduce the effects of these risks.

The standard is separated into two parts, with the first part containing 10 clauses, and the second part, called Annex A, outlining 114 controls. Clauses 0-3 are the introduction to the standard and include the **'Introduction', 'Scope', 'Normative references'** and the **'Terms and definitions'** section in that order. Clauses 4 through 10 include:

Content of the Organisation

This section defines the business, including any interested parties, external or internal issues, and any other needs that should be considered.

Leadership

The commitment of senior management to the ISMS is integral to its success. This section includes laying out the objectives, creating and communicating the information security policy, and the provision of resources and support from management to those implementing the system — as well as assigning roles and responsibilities.

Planning

At this stage, an information security risk assessment is developed that feeds into security objectives that are also aligned with the overall business goals. This is then clearly communicated to the entire organisation. A risk treatment plan is also created.

Support

Competence, awareness, communication, and resources are important when implementing the system, so training needs to be provided. All information needs to be documented and kept up to date to maintain the ISMS.

What is **required?** *(continued...)*

Operation

Processes to mitigate risk need to be planned, implemented, and controlled. Risk management can then be put into action.

Performance Evaluation

Monitoring, measurement, and analysis of the ISMS in action is integral to its success. This includes regular internal audits and senior management reviews.

Improvement

Continuous improvement is the foundation of the framework, and therefore evaluation must be followed up by improvement - with any noncompliance rectified.

Annex A (Statement of Applicability)

This section contains the controls and measures that will be put in place as derived from the risk assessments. These consist of technical, organisational, legal, physical, and human resource controls.

The 114 control areas include:

- Information security policies
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

ISO 27001 certification is advantageous in more ways than one...

- ✓ Through the strengthening and bolstering of your current system, **improve information security across your business.**
- ✓ **Boost business resilience** by assessing, managing, and mitigating risks posed to information security through better processes and security strategies.
- ✓ **Qualify for tender applications and frameworks** that stipulate that ISO 27001 certification as a “must have”.
- ✓ **Achieve preferred supplier status** by evidencing your commitment to data protection and **demonstrating compliance.**
- ✓ Showcase the accreditation to **increase new business opportunities** and **win new customers,** as well **retaining current clients.**
- ✓ **Boost your competitive advantage** and improve your brand reputation by gaining certification and proving that you take information security seriously.
- ✓ **Promote a culture of continuous improvement** through the implementation and maintenance of the ISMS.

So what are you waiting for? Speak to us today and start working towards these fantastic benefits.

Achieving ISO 27001 in just five steps

Achieving ISO 27001 certificate is easier than you might think, especially with the support of Synergos from start to finish.

Step 1:
Develop your ISMS

Establish your ISO 27001 Information Security Management System, gaining buy-in from the entire business. This includes examining your current procedures, carrying out risk assessments, identifying risks and opportunities, and developing controls.

Step 2:
Appoint a UKAS accredited certification body

A UKAS accredited body is guaranteed to be impartial, and is the gold standard for certifying bodies in the UK.

Step 3:
Review your ISMS

Carry out a thorough review of the system and ensure that you have all the assets and documents in place ahead of your stage one audit.

Step 4:
Complete your stage one and state two audit

An auditor will visit your site to carry out the stage one audit, providing recommendations and amends to be rectified before returning to carry out the stage two audit — resulting in certification if it meets the standard.

Step 5:
Maintain the ISMS for annual review

To ensure continuous improvement, a UKAS auditor will return annually to review the ISMS and recertify your business.

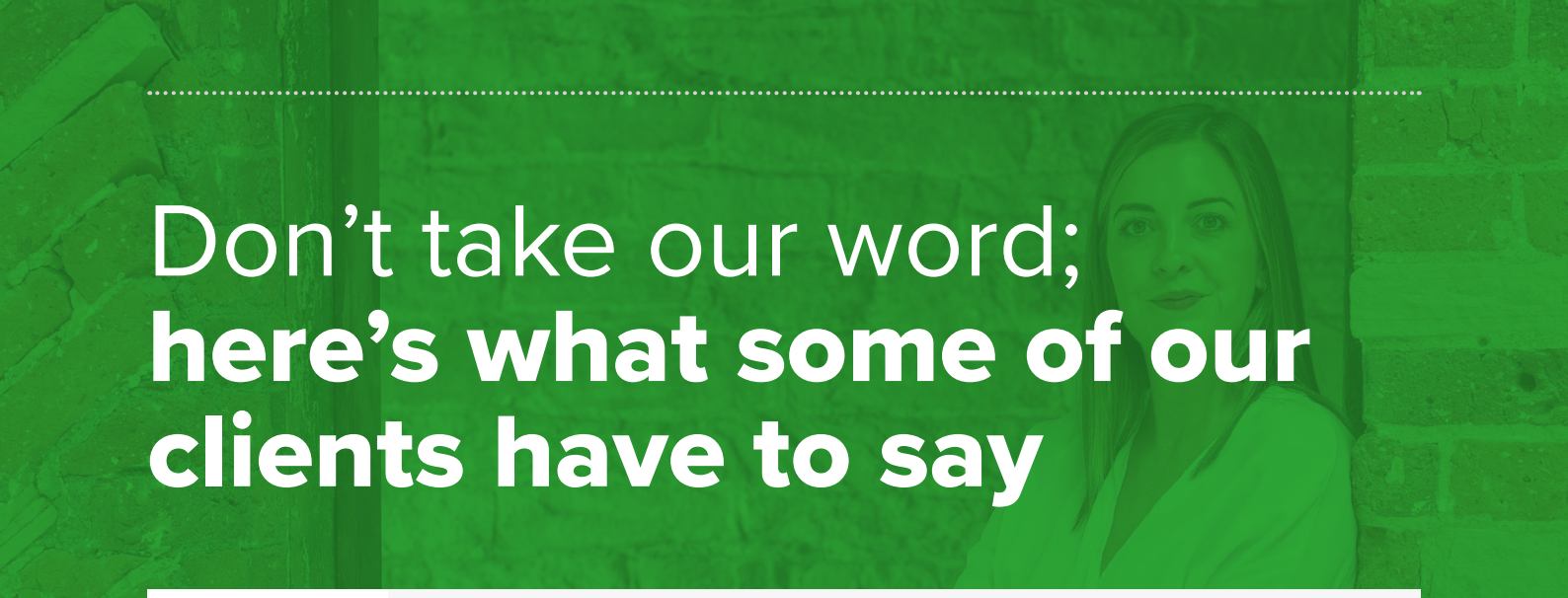
Our expert team can help and guide you every step of the way, so get in touch today to discover more.

Book an appointment now

Why choose Synergos?

Our team of expert, reliable, and approachable consultants will have you soaring through the process in no time! And, we also offer:

- ✓ **A 100% guarantee that you will achieve your chosen certification,** or we will refund the entirety of the monies paid to us, as per our terms and conditions. That's how confident we are that we can help you gain ISO 27001 accreditation.
- ✓ **We'll manage the entire process for you,** so you can focus on your day-to-day business operations.
- ✓ Ongoing support, to ensure that your Information Security Management System is maintained and up-to-date to **ensure recertification during your annual audits.**
- ✓ **We've a proven track record** of helping our clients to achieve their certifications — so you can be confident in putting your trust in us.



Don't take our word; **here's what some of our clients have to say**

"Synergos understood our challenges, as well as the restrictions and resources within our business. Her knowledge, reassurance, approachability, and availability all factored in the final decision The ISO was a fast process, and the consultant was there to support right from the beginning. Documentation was provided where needed, as well as full preparation and support focused on the key requirements. We will certainly continue to recommend Synergos — even to our own clients."

Catherine Embleton, Office Manager, Concept IT Services Ltd

"Achieving ISO 27001 certification is recognition of the hard work our team do to ensure the highest standards, and it was invaluable to work with the compliance experts at Synergos deliver an efficient process."

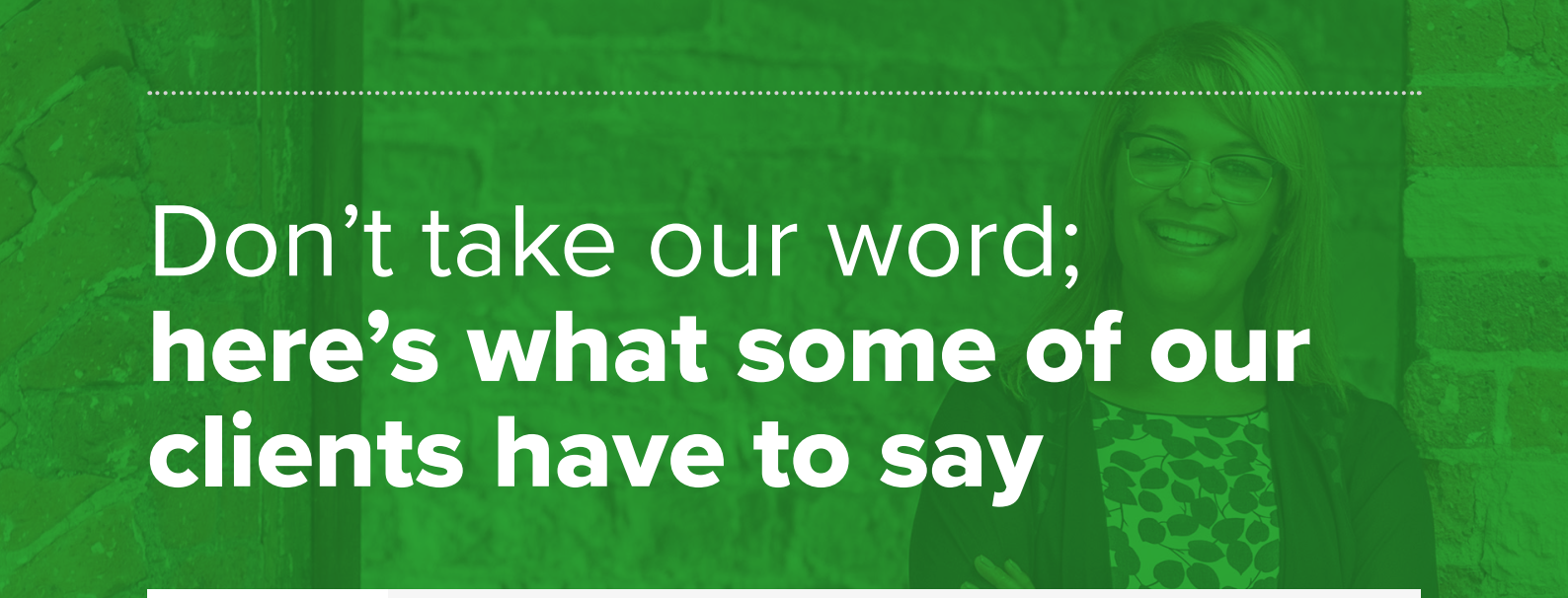
Nigel Garner, CTO Director, Answer Digital Ltd

"Synergos is absolutely fantastic at what they do!

They help translate technical jargon into understandable information. They are all incredibly knowledgeable of all areas of compliance!

They offer a professional, responsive, and great quality service which was paramount to us being recommended for certification!"

Liam Fitzakerley, Compliance Manager, Skanwear Ltd



Don't take our word; **here's what some of our clients have to say**

"Delighted to be working with Jenny and her team - great partnership approach, understanding and recommending solutions to fit our business. Always friendly, approachable and professional we would highly recommend their services to other companies wishing to go through the ISO process and certification."

Gail Weathers, Director, resource Ltd

"We use Synergos for the ongoing management of our Information Security Management System and to ensure we stay ISO 27001 certified.

I can honestly say that Synergos has comprehensively taken over the responsibility of our ISMS and assumed all roles that an Information Security Manager has so successfully that I don't have to worry about a thing. It's made my life so much easier and helped us to enhance what we already have in place.

I would 100% recommend Synergos to anyone who is considering outsourcing their ISO 27001 requirements."

Sim Hobson, Project Manager & Co-Founder, Steamhaus

"Appointing Synergos to help us manage our ISO credentials and ensure we're managing our policies and our systems properly was the best decision we made last year. And I'm pleased to say that we have just passed our ISO accreditation for another year. It's incredibly reassuring knowing we have Steve to turn to and it's great having someone who helps turn all the formalities into something we can understand!"

Moira Throp, Director, like minds Ltd

We hope you found this overview useful. If you have any queries or want to begin your ISO 27001 journey to enjoy all the benefits it brings, contact us today for a no obligation, informal conversation.

SCL SYNERGOS CONSULTANCY LTD

01484 666 160

team@synergosconsultancy.co.uk

www.synergosconsultancy.co.uk

Unit 18 Office T1 Brooke's Mill Office Park, Armitage Bridge Huddersfield, HD4 7NR