



ISMS.online

Achieve your first ISO 27001

Your guide to fast and
sustainable certification

- 5** What is ISO 27001?
- 7** Why is ISO 27001 so important?
- 8** Building trust
- 11** More than cybersecurity
- 12** How do you get there?
- 14** Why do you need an ISMS?
- 16** Your ISMS should work for you
- 19** Get a 77% headstart
- 20** The days of the static ISMS are long gone
- 22** Kick off with confidence
- 23** Specialist support
- 25** Ace your audits
- 27** About ISMS.online

So, you need to get ISO 27001 certified.

If this is your first experience with the internationally recognised standard, you're probably wondering how to get started.

In fact, you might even be feeling a little overwhelmed. That's understandable. It's a big standard with a lot of interconnected parts. Don't worry. We help organisations all over the world with the most practical, affordable path to achieving and maintaining their ISO 27001 certifications, every single day. It's what gets us up in the morning!

In this guide, we'll help you understand:





What is ISO 27001?

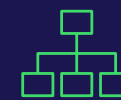
ISO 27001 is the only truly global information security standard, so naturally it's one of the most widely sought-after.

It's applicable to every industry and it sets out how to design, build and implement an Information Security Management System (ISMS) that can be independently certified for assurance purposes.

The ISO 27001 standard has been designed by ISO, the International Organization for Standardization, a network of national standards bodies covering most countries in the world.



Internationally recognised best practice standard for information security management systems (ISMS)



A framework to assist organisations in protecting the Confidentiality, Integrity and Availability of their most valuable assets



Provides a risk-based approach to information security management







A continuous improvement process (Plan/Do/Check/Act) to ensure ISMS remains relevant



Why is ISO 27001 so important?

In today's threat heavy landscape, ISO 27001 offers you the best possible protection for your information assets. But it does so much more.

Powerful customers and security-focused supply chains are increasingly viewing ISO 27001 certification as a baseline requirement for doing business. It's no longer a 'nice to have', it's an expectation.

-  **Reduce information security risks**
-  **Win new business**
-  **Defend existing contracts from competitors**
-  **Save time and money through improved practices**

Building trust

Trust is one of the keys to success for any business.

And that’s one reason why more and more companies are choosing to get ISO 27001 certified, so they can demonstrate that they can be a trusted partner to their customers and supply chains. In fact, certifications in ISO 27001 have risen by 450% over the last 10 years.

If you’re not planning to get certified then your competitors are.



DISTRUSTED

TRUSTED



Some customers choose not to get certified, usually because of cost. They still need an ISMS that is easily managed and accessible to interested parties - and one that can easily be used to achieve certification if they change their minds



More than cybersecurity

Contrary to popular belief, ISO 27001 is not a security standard but a management standard. It's a framework designed to help you identify a risk level that is tolerable to your operations, and that of your wider supply chain.

ISO 27001 covers information security, physical security, cybersecurity, business improvement, business development and data privacy.

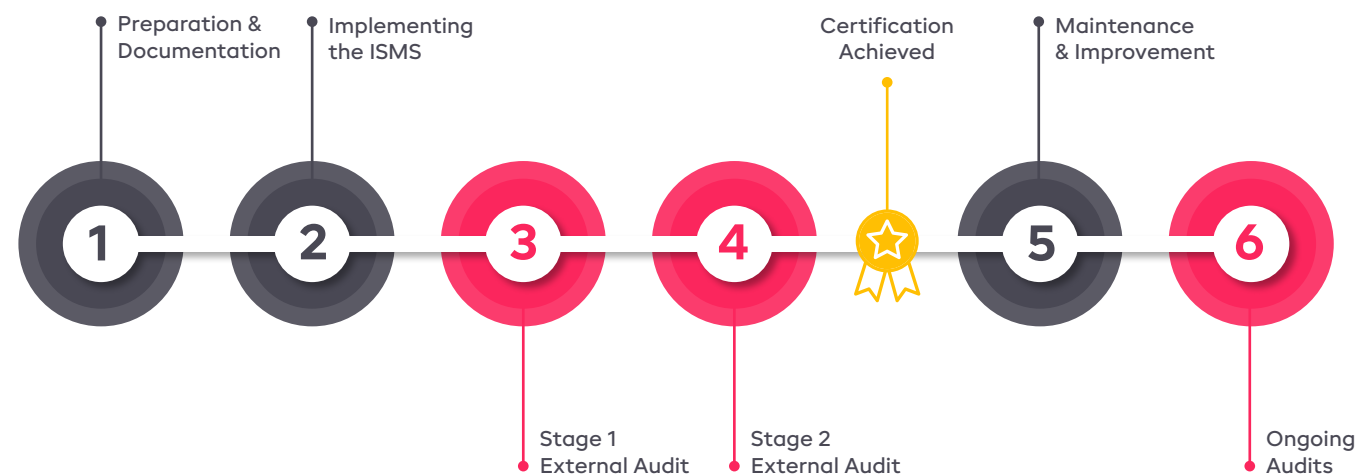
The standard delivers a risk-based framework for those elements and exists in two parts: **Clauses** and **Annex A** controls.

Clauses 4-10 detail the scope, definitions and requirements you'll need to consider when implementing and maintaining your ISMS.

Annex A provides over 110 objectives and controls, divided into 14 categories. These are the levers you put in place to manage and mitigate risk to your organisation and its supply chain.

How do you get there?

To achieve ISO 27001 certification you need to create an ISMS that follows the ISO 27001 standard. Then you must successfully pass through two external audits so your auditor can recommend you for certification to the relevant accreditation body. That certification lasts for three years, with further internal and external audits along the way.



ISO 27001 success takes commitment from everyone in your organisation. Exactly how much differs depending on the decisions you make around Clauses 4–10, as you:



Align your ISMS with your business strategy



Identify your business information assets



Decide the scope of your ISMS

“ Thanks to ISMS.online, we achieved ISO 27001 UKAS certification within four months. I can honestly say we wouldn’t have been able to do it without ISMS.online and their support team.

DEAN FIELDS
IT Director, NHS Professionals

NHS
Professionals

Why do you need an ISMS?

You need an ISMS because without one you won't achieve ISO 27001. It's an essential part of the compliance and certification process.

That's because it demonstrates your organisation's approach to information security. It defines how you identify and respond to opportunities or threats relating to your organisation's information and any related assets.

After all, the clue is in the title. The only way of showing you're managing your information security properly is by having your information security management system in place!

“ We needed ISO 27001 to win new corporate clients and we needed it quickly. ISMS.online gave us a one-stop solution that radically speeded up our implementation.

EVAN HARRIS
COO, Peppy

Peppy™

Don't invest in a traditional ISO 27001 gap analysis

We'd advise steering clear of a traditional gap analysis. Pre-configured services like ours offer a great head start, closing many common gaps immediately. Invest in one of them instead to achieve an immediate return and save valuable time and effort.

Don't rely on a document toolkit and a shared drive folder

An ISMS includes actionable documents and spreadsheets. But that's only part of what you'll need. It should also be visible, transparent and easily accessible to authorised parties. That's impossible to achieve with just some basic documents and old-fashioned folders and drives.

An ISMS is for life and you need to show you live it

Your ISO auditors will ask for evidence of ongoing management including reviews of ISMS policies, controls, assets, risks etc. You'll also have to show you're carrying out internal audits and improvement or corrective actions.

Don't divert valuable resources into building your ISMS from the ground up

Building an ISMS from scratch is like developing a bespoke sales or accounting system. Your organisation will have to devote considerable time, effort and budget to delivering systems and services that are readily available in existing off-the-shelf products.

Your ISMS should work for you, not the other way around.

Not all ISMS are created equal. If your ISMS doesn't have these characteristics as an absolute baseline, you'll end up with a less effective ISMS and working much harder than you need to.

- ✓ **All-in-one-place working**
Make sure you choose a single software solution that's futureproofed for your ongoing compliance needs.
- ✓ **Security confidence**
You'll hold some very sensitive information in your ISMS so avoid software solutions with weak security.
- ✓ **Always accessible**
Your ISMS should be available to authorised parties securely, when and where they want it, with backup and support as needed.
- ✓ **Easy to use**
Keep it simple – complicated management systems are costly to use and encourage noncompliance.
- ✓ **Structured for success**
Ensure your software supports discipline and timely progress while being flexible and scalable.
- ✓ **Joined up**
Choose a solution with easy navigation and workflow linking to help stakeholders find their way.
- ✓ **Transparent**
Impress your auditor with an ISMS that shows your working as it evolves, making it easy to record and track changes.
- ✓ **Collaborative**
Go for built in collaboration tools to avoid duplication and help to demonstrate continual improvement.
- ✓ **Insightful and actionable**
An ISMS with pre-configured reporting and reminders will help you and your stakeholders make better decisions.
- ✓ **Affordable**
Prove your return on investment with an ISMS that's cost effective to implement and operate.

Get a 77% headstart

Our Adopt, Adapt, Add (AAA) philosophy means your information security management system is quick and easy to implement, in fact you'll have made up to 77% progress the minute you log on.

Our platform comes preconfigured with tools, frameworks, policies & controls, actionable documentation and guidance to meet every single ISO 27001 requirement and Annex A clause.

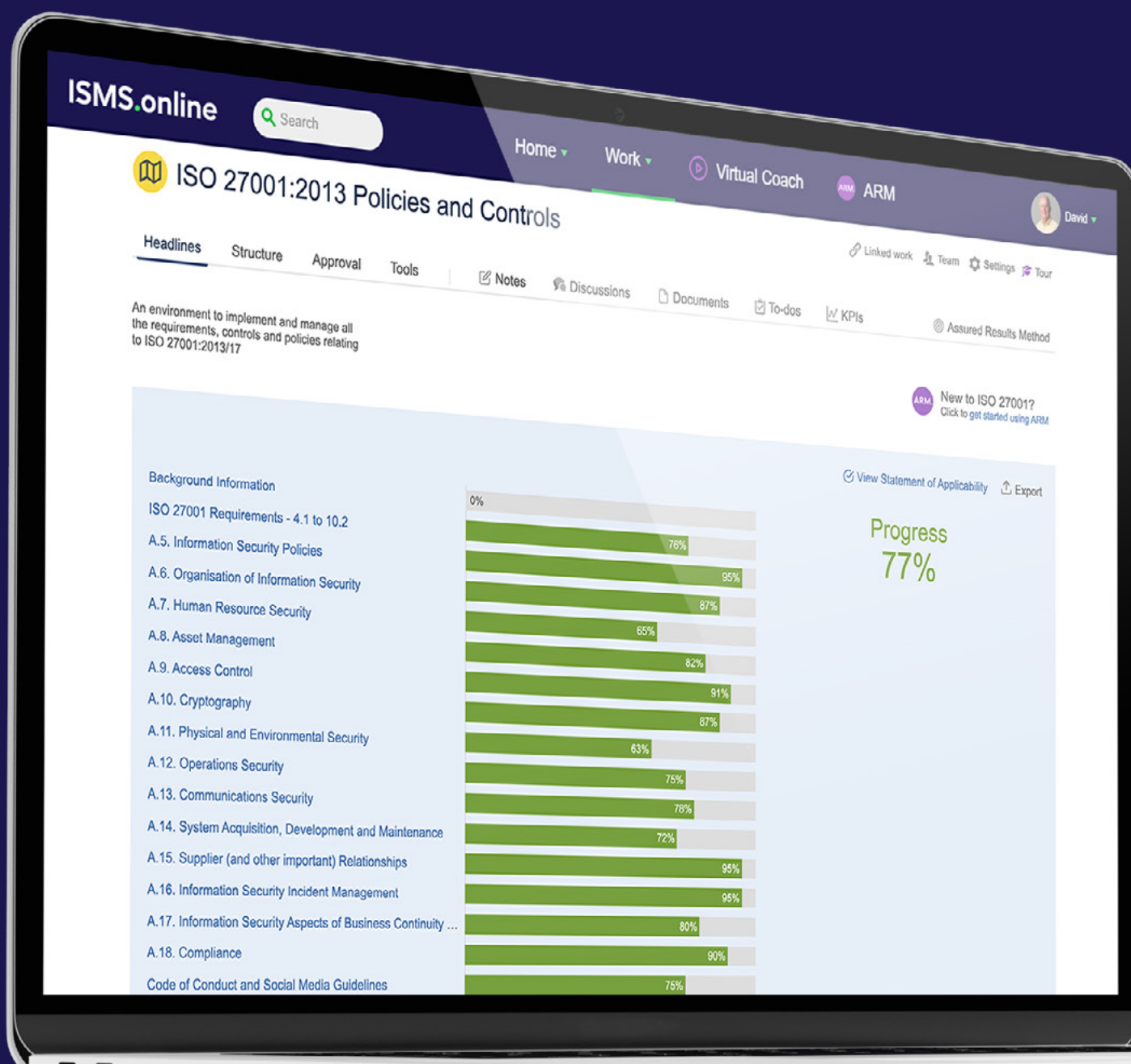
You can simply:

- **Adopt** it, if you don't already have anything in place
- **Adapt** any of them easily to fit in with your existing way of working
- **Add** any specific policies and controls to meet your organisation's unique needs

“ I certainly would recommend ISMS.online. It makes setting up and managing your ISMS as easy as it can get.

PETER RISDON
CISO, Viital

viital



The days of the static ISMS are long gone

Disconnected templates and toolkits supported by an expensive consultant just don't cut it anymore.

Your ISMS is a fundamental enterprise-wide system. As much a cornerstone of your operations as your CRM, HR or accounting software. You wouldn't build those yourself, so why would you build your own ISMS?

We've developed a series of intuitive features and toolsets within our platform to save you time and ensure you're building an ISMS that's truly sustainable. So once you've achieved your first certification, re-certification is as easy as 1, 2, 3.



Policies & Controls Management

Easily collaborate, create and show you are on top of your documentation at all times



Risk Management

Effortlessly address threats & opportunities and dynamically report on performance



Measurement & Automated Reporting

Make better decisions and show you are in control with dashboards, KPIs and related reporting



Audits, Actions & Reviews

Reduce the effort and make light work of corrective actions, improvements, audits and management reviews



Mapping & Linking Work

Shine a light on critical relationships and elegantly link areas such as assets, risks, controls and suppliers



Interested Party Management

Visually map and manage interested parties to ensure their needs are clearly addressed



Documented Procedures

Simply document, easily control and publish your procedures to ensure stakeholders follow them



Other Standards & Regulations

Neatly add in other areas of compliance affecting your organisation to achieve even more for less



Staff Awareness & Compliance Assurance*

Engage staff, suppliers and others with dynamic end-to-end compliance at all times



Supply Chain Management*

Manage due diligence, contracts, contacts and relationships over their lifecycle



User Management & Permissions*

Practical permissions with low cost plans for more regular and occasional users



Privacy & Security

Strong privacy by design and security controls to match your needs & expectations

*optional add on

Kick off with confidence

The implementation part of the journey is often the most challenging and misunderstood. That's why we've built ISMS.online with optional features that will save you time and help you navigate the process with ease and confidence.

ARM

Assured Results Method

ARM is your simple, practical, time-saving path to first-time ISO 27001 compliance or certification. It breaks the whole process down into simple steps and guides you through them one by one.

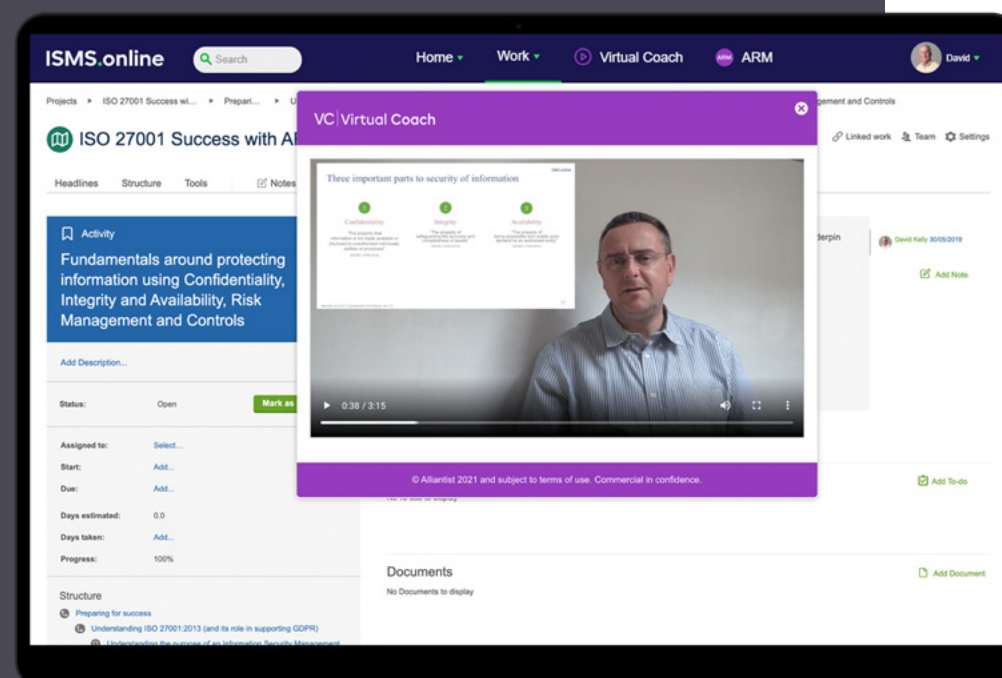
100%

of our customers who have used ARM have achieved certification on their first attempt

VC

Virtual Coach

An 'always on' set of videos, checklists other guides focussed on the 'what, and how' of ISO 27001. It demystifies part of the journey for implementation ongoing management.



Specialist support

You're busy and ISO 27001 is a big subject, so you may experience gaps in your capability, capacity or confidence. As an ISMS.online customer you have unlimited access to a Live Support Team of platform experts and a dedicated Customer Success Manager who has a stake in your success.

During your onboarding we help you identify what you currently have, what you may be missing and how quickly you're looking to achieve your goals. The outcome is a personalised roadmap that you can reference to ensure you're staying on track. If at points you lack the discipline to stay on target, our team of in-house specialists can step in to temporarily lighten the load.

“ ISMS.online is an indispensable helper on the ISO 27001 certification journey, with a mix of great software and an experienced support team.

OLGA VOVK
Head of QA, Generis



“ The feedback we got from our auditor was that it was the easiest audit they’d ever done.

ALLEN KNIGHT
CEO, Taxlab



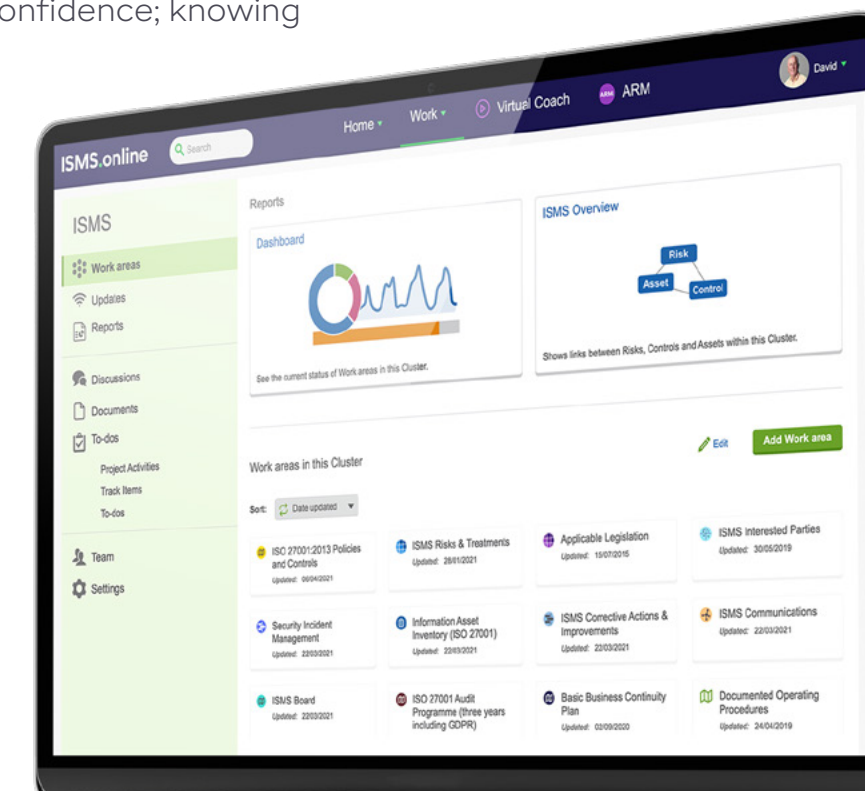
CHOOSING YOUR CERTIFICATION BODY

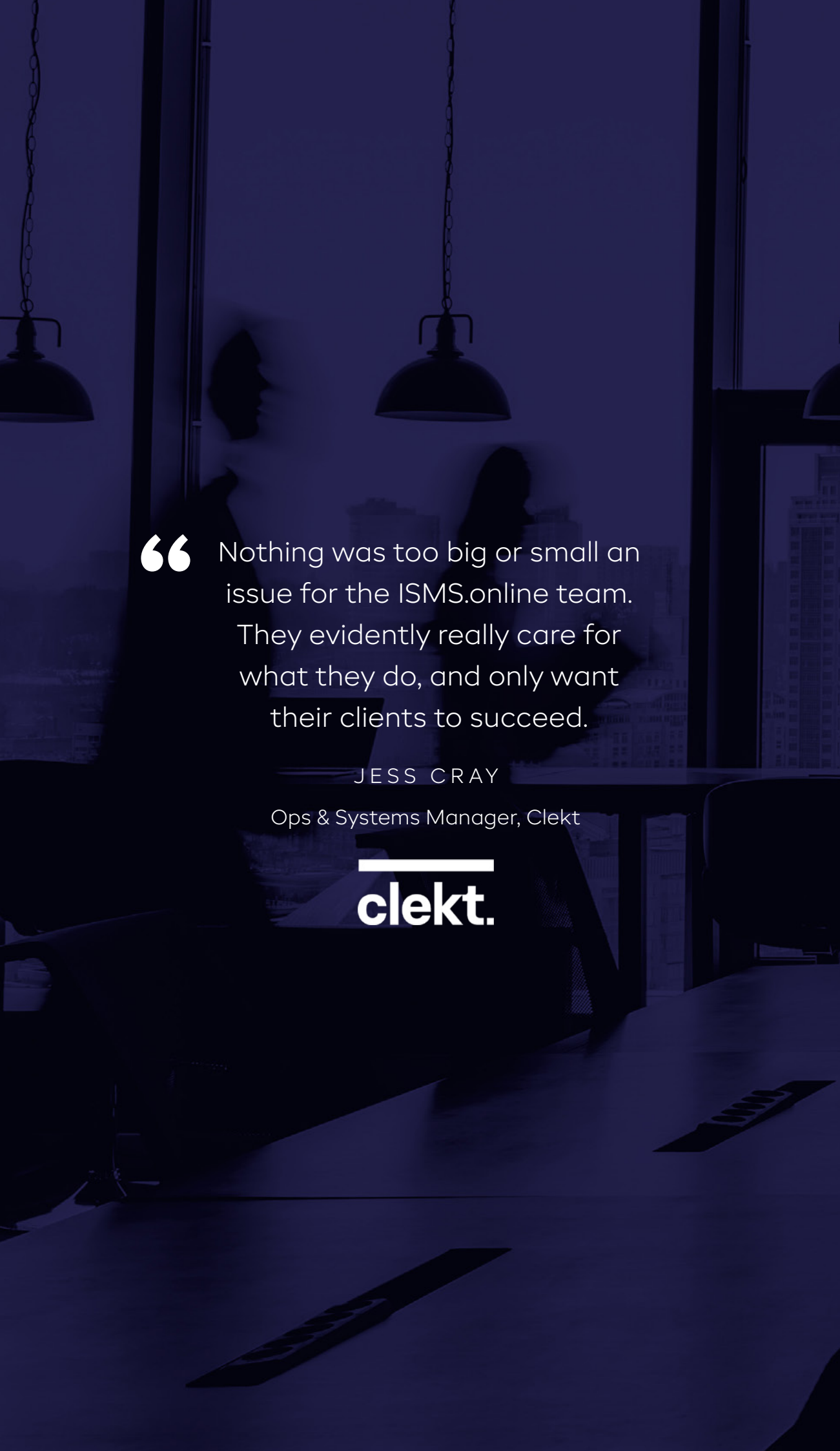
Not all certification bodies are the same so choose wisely when you’re looking for an independent audit of your ISMS. We can help you choose a trusted certification partner that will satisfy the most demanding of customers.

Ace your audits

With your ISMS all-in-one-place and instantly accessible, you’re perfectly placed to demonstrate the ‘process of continual improvement’ required by the foundational ISO 27001 standard.

Our collaboration and project management tools ensure your compliance becomes ‘business as usual’ with all your activity creating clear audit trails. You’ll approach every audit with confidence; knowing you’ve removed the risk of human error while saving time and reducing cost.





“ Nothing was too big or small an issue for the ISMS.online team. They evidently really care for what they do, and only want their clients to succeed.

JESS CRAY

Ops & Systems Manager, Clekt

clekt.

About ISMS.online

When our parent company Alliantist set out to achieve ISO 27001 certification some years ago, it found the process more complicated, time-consuming and expensive than first anticipated.

There had to be a better way. Something practical, affordable and accessible to interested parties, something ‘all in one place’. It didn’t exist, so we decided to create it.

That’s when ISMS.online began.

Since then, we’ve helped organisations all over the world with the most practical, affordable path to achieving and maintaining ISO 27001 compliance and certification. Along the way we’ve evolved to help you overcome all your governance and compliance challenges. So, once you’ve achieved success with ISO 27001 it’s easy to expand beyond information security into privacy and business continuity too.

We have helped hundreds of organisations of every size achieve ISO 27001 certification first time.

If you’d like to see how we can help you then just book a demo today and we’ll be happy to help.

Book a demo today

ISMS.online

Still got questions?

Our expert advisers can help:

enquiries@isms.online

Or join the conversation on our socials



HM Government
G-Cloud
Supplier



Member
CyberExchange



TECH NATION
CYBER

