Achieving your first ISO 27001 certification

ISMS.online

Turning trust into certainty

The right path

There are many reasons to achieve ISO 27001, the global standard for information security management. But we've found that our clients are often driven by two key drivers.

1. Internal e.g. Senior management are seeking business improvements or responding to one or more incidents that have caused or could have caused reputational or financial issues.
2. External e.g. It's a requirement from existing or potential customers, or it's recommended/accepted as an industry standard to make their organisation safer, more resilient and more successful, and a price of entry into the sector.

If you only have internal drivers, you may decide that compliance is fine initially. External drivers are more powerful than internal, especially for an independent certification.

That's certainly what drove us when we set out to achieve ISO 27001 success for Alliantist, ISMS.online's parent company, some years ago. But the process was more complicated, time-consuming and expensive than we thought it would be.

We looked around for help, but we couldn't find the practical, affordable, all-in-one place support we needed. So we decided to create our ideal information security management system (or ISMS) ourselves. That's how ISMS.online began.

Now we help organisations all over the world with the most practical, affordable path to achieving and maintaining ISO 27001 **confidence in compliance** and **certification with certainty**. And of course, we have everything you need all in one place.

In this guide, we'll show you how we do that. But first of all, we'll show you why it's so important. We'll help you understand what good information security management looks like and see how ISO 27001 can help you fulfil your promises to your clients.

In short, we'll show you how to take the trust people already have in you and turn that into ISMS certainty.

Contents

What's ISO 27001 and why do you need it?

ISO 27001 is one of the world's most popular information security management standards. It's the only standard that sets out how to design, build and implement an Information Security Management System (ISMS) that can be independently certified for assurance purposes. It's applicable to every industry and is increasingly required to do business.

Why? Because organisational and supply chain risk is growing, and regulation is on the increase. The financial and reputational consequences mean senior leaders can no longer take information security on trust. They need certainty, both within their own organisations and from their suppliers, partners and even their customers. That's led to widespread adoption of ISO 27001, the internationally recognised best practice framework for information security management.

In fact, an independently certified ISO 27001 ISMS is increasingly the minimum expectation for satisfying external stakeholders. But not all ISO 27001 implementations create the same level of certainty.

There are differences between compliance and certification, and there are some bodies who are trusted more than others to offer an independent audit of your ISMS. And of course, it's very important to make sure your ISMS stays effective once it's in place.

That's why we do far more than help you develop a new ISMS. If you need to satisfy external parties, like major customers or partners, we'll help you choose and achieve the right certification. And once your ISMS is up and running, we'll offer long term support to help you keep your information secure in this ever-changing world.

Invest in an ISMS to achieve ISO 27001 certification and:

- ✓ Reduce information security and data protection risks that can cost your organisation much more in reputation, fines or rework
- ✓ Win new customers and retain existing business in an increasingly distrusting world
- ✓ Save time and money by improving business practices internally and across the supply chain

Tips

Calculate your ISMS ROI by adding the benefits of:

Addressing opportunities and threats + Meeting stakeholder expectations

And subtracting the costs of:

Steps to overcome pushback + People & tech setting up and managing your ISMS

This is a very topline summary. To find out more about ISMS benefits, costs, challenges and returns, download our ISMS business case whitepaper

What’s an ISMS and why do you need one?

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 describes and demonstrates your organisation’s approach to information security. It defines how your people, policies, controls and systems identify and respond to opportunities or threats relating to your organisation’s information and any related assets. After all, the clue’s 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!

Four key tips for ISMS development

1

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.

2

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.

3

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.

4

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.

How will your ISMS achieve ISO 27001 certification?

To achieve independent ISO27001 certification, your ISMS will need to pass a two-stage audit.

That audit will be conducted by a recognised certification body, accredited by the International Organization for Standardization (ISO). Stage 1 assesses its documentation and Stage 2 looks at how it works in practice, testing it through interviews and sampling.

That's followed by ongoing surveillance audits, which usually take place at least annually. Your certification will last for three years, with a recertification requirement in the third year. This route is slightly more expensive than self-certification or audits by independent consultants, but it's usually the only way to be taken seriously by smart customers and regulators.

What do you have and need for success now?

			Internal driver	External driver
1	2	3	4	5
Has no information or cyber-security management people, systems, policies or technology in place	Spends minimum time on security related policies, but they're not structured as a system and don't follow any standards	Meets the requirements for basic information security management, e.g with Cyber Essentials	Invests in people, policies, processes and systems to show compliance with ISO 27001, and has an information security management system (ISMS)	Has achieved and maintains an independently certified ISMS that follows ISO 27001, underpinned with a sustainable technology solution
Distrusted				Trusted
Not an ISMS	Not an ISMS	Not an ISMS	ISMS.online offers **visible confidence in compliance** and can be audited or demonstrated easily to their end customers and other stakeholders where the organisation chooses not to achieve independent certification (e.g. because certification is costly)	ISMS.online underpins independent **certification with certainty** and is easier to certify at lower audit cost (for internal and external time)

Referencing this heat map, where would you place your organisation today? Unless you have an ISMS (stage four or five) you can not prove you are ISO 27001 compliant let alone certified.

Stage four is ideal if you only have an internal driver. You can also save on costly external certification fees until such times as the external drivers become compelling for a level five independently certified solution.

For some stakeholders even that fifth stage is just a starting point because they need more than trust. That's because trust is always a choice. Like them, we believe in stepping beyond it to create clear and specific certainty.

Why certainty? It's based on clearly defined behaviours and actions, and concrete achievements. It's about knowing facts, not believing in possibilities. To achieve maximum impact, your ISMS should be built on certainty. It should assure your certification success and give your stakeholders specific factual proof of your resilience and durability.

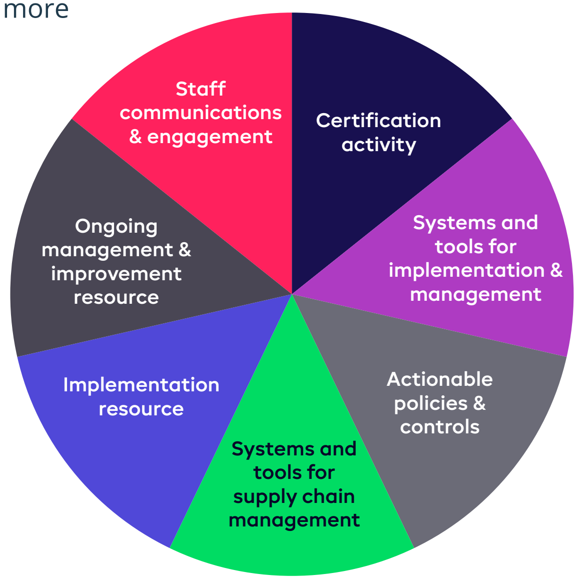
What's included in an ISMS?

An effective ISMS is made up of the seven elements shown in the pie chart below. The time and cost required for each slice depends on your objectives, your starting point, the scope of your ISMS and your organisation's preferred way of working.

Higher levels of staff engagement and compliance help make ISMS success more likely.

Achieving recognised, independent ISMS certification increases external stakeholder certainty.

High investment in one slice will bring down the cost of other slices. For example, using off the shelf Software-as-a-Service (SaaS) technology and actionable documentation will drive down implementation cost and time. It will also bring down ongoing management or improvement resource needs and costs over the life of your ISMS.



Effective control and collaboration within your supply chain can reduce risk and cost while improving business continuity and overall resilience.

The practical systems and tools for implementation and management of an ISMS include:

- Policy Creation, Management and Governance, including regular reviews and evaluation capability
- Information Asset Inventory
- Risk Management & Other Decision Support Tools
- Statement of Applicability reporting and insight
- Internal auditing, management review and reporting functionality
- Performance improvements, corrective actions and measurements against objectives
- Security event, weakness and incident management
- Supply chain management
- Business continuity management
- Staff awareness, communications and engagement as well as HR lifecycle security
- Ideally the ISMS will be able to link up to other standards and regulations to increase efficiency, whilst reducing overlap and confusion for the parties involved.

Not all ISMS software is the same

A credible ISMS solution will impress powerful stakeholders. It will speed time to success, improve visibility, ease coordination, reduce risk, lower the total cost of ownership and lead to greater certainty. The right ISMS software will make all the difference too.

Choosing the right ISMS software also helps the people who will administer your ISMS, making it easier to address any confidence, capability, capacity or discipline issues. That's particularly important when they're new to information security management or can only devote part of their time to it due to other responsibilities.

We've identified 10 characteristics that underpin the best ISMS software. ISMS.online meets all these characteristics. We'd encourage you to test your other options to see if they do too.

1. All in one place working

People are busy. They don't have time to learn and use lots of different systems. Deploying multiple systems also increases search, knowledge management, coordination and contracting costs. And it creates risk, time and complexity challenges.

Make sure the software you choose comes ready-configured with all the features and functionality for the standards and regulations you want to achieve. Factor in flexibility for future-proofing too.

2. Security confidence

You'll hold some very sensitive information in your ISMS. So avoid software solutions with weak security, which can lead to confidentiality, integrity or availability issues. Look for software or provider credentials like:

- UKAS certified ISO 27001 application, organisation and supply chain (not just data centre)
- Independent penetration test certificate/s for the application and its infrastructure
- GDPR compliance confidence to ICO levels
- Strong security settings including: 2 factor authentication and Single Sign On (SSO) options

3. Always accessible

Your ISMS should be available to authorised parties securely, when and where they want it, with backup and support as needed. Making your ISMS available to any secure location at all times will help you:

- Work where and when you want to
- Hit your goals and targets more quickly
- Demonstrate and build confidence in your ISMS during customer meetings
- Manage your ISMS in real time when needed - for example after a security incident or when triggering a business continuity plan

4. Easy to use

Not everyone's a full-time expert. People move on. Relying on one person to manage your ISMS will put your business at risk. Complicated management systems can also create higher costs of use and drive noncompliance with some or all processes. So, look for software that's easy to learn, understand and use.

5. Structured for success

With lots of work involved in an ISMS, having a structure to follow and discipline in the planning & delivery of it makes execution easier. Seeing progress being made enthuses users too. Being able to adapt and add to that over time is also important to future proof and avoid rework.

So, make sure your solution supports discipline, progress and timely action whilst being flexible, extensible & scalable for a fast-changing world.

6. Joined up

The person doing some of the ISMS input work may not be the same person who benefits from or reviews it. Easier navigation through and linking of workflows reduces cost and gives stakeholders confidence that the ISMS fits together as it should.

7. Fully transparent

Trust is default 'low', with stakeholders wanting evidence of work done, including visibility of changes over time. So we recommend choosing an ISMS that helps you show your working as it evolves in line with business changes. Make sure it lets the changes you make and the information you record be visible, auditable, clearly approved and evidence-based.

8. Supports collaboration

Modern employees rarely work alone internally, and increasingly collaborate externally too. Without collaborative features embedded inside the ISMS, costs of coordination and sharing can be high. That can also create gaps in the ISMS or duplication across other systems. So be sure to confirm that the system you're looking at allows for the right level of collaboration.

9. Better decision support

Stakeholders want to see and know that your ISMS is under control. The best ISMS solutions should drive down the cost of reminding and reporting, freeing people up to make better, more timely decisions. Look for a solution that includes dynamic reports and reminders. They'll automatically do the heavy lifting, helping you avoid admin or rework costs.

10. Affordable

A well-run ISMS, addressing key threats and opportunities, creates high returns. But the cost of the people and technology that run it needs to be justifiable relative to the value at risk. So, make sure that your total ISMS solution is cost-effective to implement, operate and improve.

Introducing ISMS.online

ISMS.online

We make our customers' organisations safer, more resilient and more attractive, helping them succeed at what they do best.

We do this primarily with ISMS.online, a secure cloud software service. It's the most practical, affordable path to ISMS certainty, with everything you need all in one place.

We also include actionable ISO 27001 documentation. It accelerates your implementation with knowledge that makes a difference. 'Out-of-the-box' you will have an online ISMS that includes a 77% head start with the requirements, policies, guidance and controls that you need for success, coupled with tools and methods that make the documentation easy to adopt, adapt and add to as required.

And if you need extra help we offer the additional services below to that make sure your organisation has what it needs for success and assurance, every step of the way.

Virtual Coach.

Virtual Coach helps you work at your own pace as you progress your ISO 27001 implementation. It's always available online, at any time, from within ISMS. online. There's no need to book courses or travel anywhere to use it. And it's the kind of competence building material that gives independent auditors confidence in your ISMS deployment.

ARM.

Our Assured Results Method (ARM) emphasises the pragmatic over the perfect, helping you build on what you already know to achieve your first certification. You can then plan for improvements over time, prioritising them from a risk perspective. Like the Virtual Coach it sits inside the ISMS. online platform, ensuring ease of access and effectiveness.

Other specialist services

If you still run into capacity, confidence, capability or discipline issues that stop you getting the results you need, we can provide bespoke practical help. Our inhouse information security experts and external partners will give you exactly the level of support you need. They're all qualified to work with ISMS.online. Whether you want a quick sanity check or deep ongoing engagement, just let us know.

Exploring ISMS.online's key features

ISMS.online is an all-in-one-place, cloud-based platform to achieve all your information security and other compliance goals, with certainty. It's the most practical, affordable path to ISMS success, whether you're new to ISO 27001 or a seasoned expert.

Policy creation, management and governance

Manage your ISMS requirements, policies and controls in one place

- Pre-built regulation, certification and standards frameworks to meet ISO 27001, ISO 27701, ISO 22301, GDPR, ISO 9001, NIST Cyber Security, NIS Regulations, DSP Toolkit, Cyber Essentials & more
- Create policies, controls, and other information quickly
- Check up on the progress and completion of your ISMS at all times
- Facilitate team collaboration
- Follow visible audit trails with version control management
- Set automated policy reminders and alerts

Information asset inventory

Replace spreadsheets with a sophisticated, easy-to-use system

- Meet the information asset inventory requirements of ISO 27001 in one secure place
- Bring your inventory to life by connecting it to risks, controls, and supply chain, and take other actions that demonstrate your assets are well protected
- Deliver GDPR requirements for a personal data inventory and show how it all joins up with your broader security protocols

Risk management & other decision support tools

Identify and address risks using dynamic, visual, collaborative tools

- Effectively manage Information Security Risks, Applicable Legislation, and Interested Parties
- Save weeks of work using our comprehensive risk bank pre-mapped to suggested ISO 27001 Annex A controls
- Dynamically link to your Information Asset Inventory, and wider ISMS
- Quickly and easily add your own risks, applicable legislation, and interested parties
- Assign and set review dates
- Treat risks, capture evidence, and retain a full audit trail
- Work dynamically alone or online in teams

Statement of Applicability for ISO 27001

An out-of-the-box SoA ready to adapt to reflect your approach

- Dynamically populate your Statement of Applicability (SoA) from within each of your ISO 27001 Annex A Control activities
- Includes standard justifications for the inclusion or exclusion of each control
- Follow the links from identified risk and relevant controls, through to the control policy itself and then to the SoA (and in reverse so that your auditor can see the risks associated with the included control too)
- Dynamically controlled to easily remain in sync with your controls as they are reviewed for inclusion/exclusion
- Share with auditors, or customers, by simply adding them as a controlled user to your online ISMS or export to physical report

Audits, management reviews and corrective actions

Meet requirement 10 of ISO 27001

- Evidence an end-to-end management of incidents and track events and weaknesses, following our proven work processes
- Filter reporting by customisable settings that include notification to regulators and victims in line with EU GDPR
- Manage and drive performance improvements using incident stats
- Handle business continuity & disaster recovery planning

Incident management

Track and manage information security incidents

- Evidence an end-to-end management of incidents and track events and weaknesses, following our proven work processes
- Filter reporting by customisable settings that include notification to regulators and victims in line with EU GDPR
- Manage and drive performance improvements using incident stats
- Handle business continuity & disaster recovery planning

Business continuity management

Protect your organisation whatever the threat

- Meet the requirements of ISO 27001 Annex A.17
- Optionally, go beyond to achieve full ISO 22301 BCMS certification too
- Track and manage Business Impact Assessments and related risks, vulnerabilities and opportunities
- Manage your incident responses in a simple but powerful workflow
- Describe your approach to ISO 22301 in a dedicated policies and controls area

Staff communication, training & awareness

Communicate, share and set tasks to meet your deadlines

- Collaborate in groups
- Set tasks for specific compliance work
- Improve learning and development
- Elevate employee engagement
- Link to policies & controls
- Demonstrate engagement for impact assessments and consultations planning

Staff & supplier compliance policy packs

Evidence that your staff understand and accept the organisation policies and processes

- Reduce policy fatigue
- One secure and accessible place to manage all policies and processes
- Evidence policies have been read and accepted
- Policy pack is sent to employees in an easy to read
- formatSet automated policy reminders and alerts

Supply chain management for information security

A joined-up approach to supplier management

- Manage supplier contracts and contacts, and capture the GDPR requirement to hold DPA’s for all relevant suppliers
- Create simple links from your ISMS to join up key risks, assets and controls affecting suppliers
- Monitor and review supplier services with a clear and full audit trail

Privacy management

GDPR Frameworks & Tools, NIST & ISO 27701

- Choose the GDPR standalone or combine with ISO 27001
- Follow the full GDPR regulation as a project framework and capture your evidence, policies and workings to demonstrate compliance
- For SME's, follow the UK Information Commissioners Office (ICO) approved self-assessment framework and capture your evidence, policies, and workings to

Human resource security

Pre-built frameworks to save you time and effort

- Complete screening and recruitment, inductions, in-life compliance, training, exit and change
- Collaborate using easy to administer teams
- Group HR initiatives together using our simple cluster functionality that makes access, navigation and analysis fast and effective

Privacy impact assessments & project management for information security

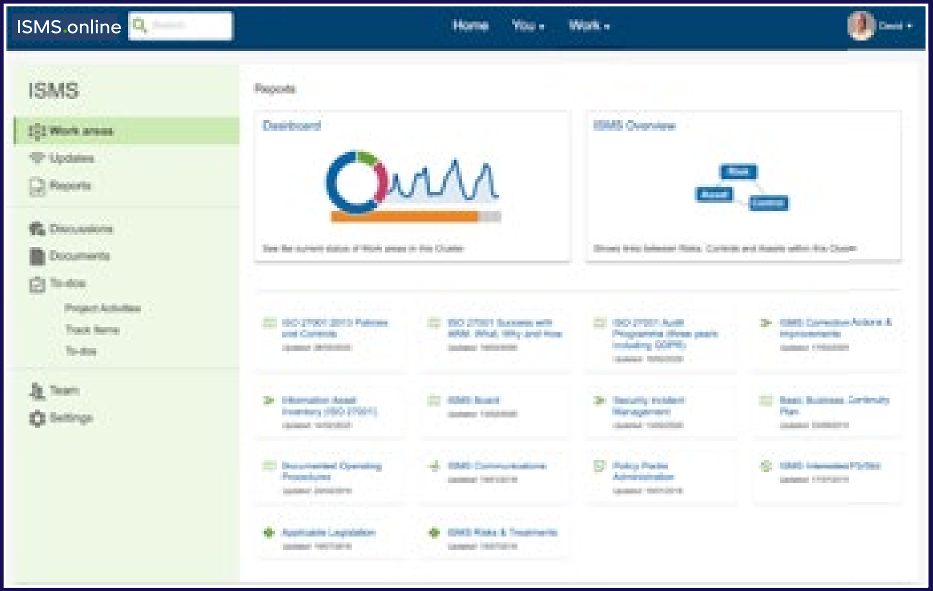
Pre-built templates to address and demonstrate your approach

- Use pre-built ISO27001 templates or build your own repeatable frameworks
- Complete project work, collaborating with colleagues in a place to evidence work
- Set KPIs and measure performance

Strategic insight from clusters & dashboards

Bring together the visual overview you need to run your ISMS effectively

Using ISMS.online clusters you can pull together any initiatives and report around them, and with each initiative area having its own automated reporting and statistics it means no more Excel, Powerpoint or wasting time on reporting performance or chasing on progress.


ISMS.online
Home
You
Work
ISMS
Work areas
Updates
Reports
Discussions
Documents
To-dos
Project Activities
Track Items
To-dos
Team
Settings
Reports
Dashboard
ISMS Overview
ISO 27001 2013 Policies and Controls
ISO 27001 Audit Programme
ISMS Corrective Actions & Improvements
Information Asset Inventory (ISO 27001)
ISMS Board
Security Incident Management
Basic Business Continuity Plan
Documented Operating Procedures
ISMS Communications
Policy Pack Administration
ISMS Interested Parties
Applicable Legislation
ISMS Risks & Treatments

Why choose us

At ISMS.online we know what it's like to be in your shoes. So we understand that an effective information security management system (ISMS) is a necessity, not a luxury. It helps you fulfil the promise of your organisation with safety, resilience and continuity planning that:

- Builds your brand and boosts your reputation by demonstrating your durability
- Helps you grow by making it easy for you to prove your security and stability
- Gives you and your stakeholders essential peace of mind

But we also know how tricky it is to achieve all that while running your organisation. So we've made it easy.

We've simplified the complex, codifying the steps and processes required to create and implement an effective ISMS, then assure your success in achieving certification for it. We'll help you maintain it too, making sure that it changes with your evolving needs and keeps on strengthening your organisation and its relationships.

We deliver our knowledge through easy to use, intuitive software. And we're easy to work with. We're open, honest and approachable.

Our partnership with you never rests. We never stop improving what we do and how we do it, as long as we're creating tangible benefits for our customers. And we're here for everyone, big or small, across the world. That's because increased global safety, resilience and continuity creates certainty that's good for us all.

We're ISMS.online. We'll help you make your organisation safer, more secure and more successful.

ISMS.online

The organisation behind ISMS.online is Alliantist Limited. It is co-owned by its staff and Cow Corner, a family firm investment business that shares the same values and beliefs.

ISMS.online was selected as one of the UK's top 20 cyber scaleups in 2019 by Tech Nation, the premier growth network for Tech businesses.

TECH NATION CYBER

Our services are all underpinned with the security and service credentials you'd expect from an organisation that takes certainty seriously. Unlike many technology providers and consultants in this space we have ISO 27001 certification internally, hold a number of key UK government security credentials and our supply chain meets or exceeds the ISO 27001 standards itself.

ISO 27001 CERTIFIED

HM Government G-Cloud Supplier

Member CyberExchange

CYBER ESSENTIALS

What our customers say

NHS Professionals

Rapid ISO 27001 certification achieved

“Since using ISMS.online, the challenges around version control, policy approval and policy sharing are a thing of the past. Our approach to risk and asset management with so many different owners has become a lot easier with everyone being able to contribute in one place.”

DEAN FIELDS

IT Director at NHS Professionals

System1 Group

ISO 27001 certification success

“We are so pleased that we found this solution – it made everything fit together much more easily. ISMS.online helps drive our behaviour in a positive way around delivering the standard in a way that works for us and our culture.”

EMMA COOPER

Managing Director, Group Operations at System1 Group

AMIGO

ISO 27001 DIY success

“The actual time invested in our ISMS implementation was probably only 2-3 weeks thanks to the massive headstart the ISMS.online platform gave us. We didn’t have to rush anything and still had the day job to do as well, so the elapsed time was around 10 months from start of the journey to UKAS certification award.”

EMMIE COONEY

Operations Manager at Amigo Technology

dubber

Global ISO 27001 certification success

“While we had an understanding of the technical requirements of ISO 27001, it was ISMS.online that helped to bring it all alive quickly with structure and pre-built tools that enabled us to embed the ISMS across our international sites ”

FRANCHERE CHAN

Information Security Lead at Dubber

ITConsilium

Straightforward decision & straightforward to use!

“We didn’t even need to demo ISMS.online to recognise that the mix of technology and knowledge were exactly what we needed to accelerate our ISO 27001 certification. It didn’t disappoint either, it’s an excellent tool and is really straightforward and intuitive to use.“

LINDEN DAVIS

Technical Director at ITConsilium

ISMS.online

Turning trust into certainty

✉ enquiries@isms.online

🌐 isms.online