Planning the business case

for an Information Security Management System

Public V1.0

For organisations serious about turning information security into business strength

Executive Summary

An effective Information Security Management System (ISMS) delivers measurable business returns.

This guide explores how to plan for that success, showing what an ISMS is, why it matters, and how to build a strong business case around it.

Information security has moved beyond a technical concern. It's now a business issue that touches every department, every partner, and every customer relationship. The complexity can feel daunting, but the path forward doesn't have to be. With the right combination of people, process, and platform, managing information security can become not only achievable but a genuine source of competitive advantage.

Whether your organisation is new to information security or already on the journey, this paper sets out a pragmatic, strategic route to success. You'll learn how to define the business value of an ISMS, make a compelling case for investment, and decide the best way to implement it, whether through internal resources, trusted partners, or platforms like IO that simplify and sustain success over time.

Throughout this guide we will explore:

- Why many organisations still hesitate to act on security, and how to overcome those barriers.
- The role of people and platform in achieving a positive return on investment, including how continuous control monitoring helps maintain assurance all year round.
- How an ISMS aligns with business strategy and builds stakeholder trust.
- Practical guidance on whether to build or buy, and how to ensure long-term value.

Information security is now inseparable from business performance. A well-planned ISMS helps organisations protect what matters, win new opportunities, and grow with confidence.

chapter one

Introduction

In this section

Three reasons why nothing happens • A point on people • In considering the technology

Cybercrime and data loss remain among the biggest threats facing organisations today, not only in financial terms but also in reputation, regulation, and resilience.

The global cost runs into the tens of millions, with impacts that can be business-ending. At the same time, privacy regulations such as GDPR, CCPA, and PIPL, alongside information security and resilience directives like NIS 2 and DORA, have raised expectations for how organisations protect, manage, and evidence the security of their data.

Despite this growing awareness, many organisations still fail to take meaningful steps to strengthen their defences. Certified frameworks such as ISO 27001, or baseline standards like Cyber Essentials, are increasingly recognised as the right foundation for good security practice, and they also make it far easier to extend into other frameworks such as ISO 27701 for privacy and ISO 42001 for AI governance as requirements evolve. Yet, adoption remains uneven, even among businesses that understand the risks.

So, why do so many businesses, even those that understand the risks, struggle to move from awareness to action?

1.1
Three reasons why nothing happens

Reason 1: No compelling internal driver

For many organisations, information security isn't seen as urgent until a serious incident occurs. Without an immediate trigger, investment can feel optional, something to revisit "later." Yet regulatory scrutiny, customer expectations, and the potential for reputational damage are growing rapidly.

Doing nothing is no longer sustainable. Regulators are tightening requirements, major customers are demanding proof of good practice in their supply chains, and even a single breach can destroy trust overnight. As these external forces intensify, leadership teams need to view information security not as a technical fix, but as a strategic priority tied directly to organisational resilience and reputation.

Reason 2: Uncertainty about what to do

The information security landscape is noisy. There's no shortage of frameworks, acronyms, and vendors with deep marketing pockets promising fix-all solutions, but for many teams, it's hard to know where to start or what will truly make a difference.

That uncertainty often leads to paralysis. Rather than taking small, practical steps towards an effective ISMS, organisations hesitate, unsure which path will deliver the right results for them.

The key is to focus on what powerful stakeholders; regulators, customers, and partners, actually expect. Following recognised frameworks such as ISO 27001 provides both structure and assurance, giving the organisation a solid foundation to demonstrate progress and maturity.

Reason 3: Seeing security as a cost, not a value driver

Too often, leaders see information security and privacy purely as an expense, necessary, but unexciting. The reality is that a well-run ISMS does far more than reduce risk: it enables growth, builds customer confidence, and reduces long-term costs.

When leaders shift from viewing information security as a cost centre to seeing it as an investment in business resilience and trust, the conversation changes entirely. Like finance systems or CRM platforms, an ISMS is an essential part of doing business well; professional, structured, and designed to scale.

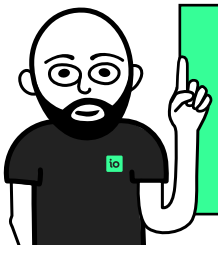
For organisations willing to take a strategic approach, the return on investment is clear.

- **Financially**, by preventing costly incidents and regulatory penalties.
- **Operationally**, through efficiency and better risk visibility.
- **Commercially**, by winning new business and strengthening stakeholder trust.

The formula for ISMS ROI is straightforward:

$$\left(\begin{array}{c}\text{Forces driving change} \\ + \\ \text{stakeholder expectations} \\ + \\ \text{ISMS benefits}\end{array}\right) - \left(\begin{array}{c}\text{People and technology costs} \\ + \\ \text{internal resistance}\end{array}\right)$$

As with any business case, increasing the value created and reducing the effort, cost, and risk required to achieve it is what turns information security from a cost centre into a genuine business advantage.



Remember this

Increase the value on the top line, reduce the friction below it. That's how information security stops being a burden and starts being a business advantage.

1.2
A point on people

Behind every effective Information Security Management System (ISMS) are capable, confident people. Technology can provide structure and visibility, but it's people who make it work.

When planning your ISMS, consider what we call the 3Cs:

- **Capacity** – Do we have the time and resources to get the work done?
- **Capability** – Do our people have the skills and knowledge to do it well?
- **Confidence** – Do they understand what's expected, and feel supported to deliver it?

These three elements determine how sustainable your ISMS will be in practice. If any one of them is missing, even the best-designed system can falter.

Many organisations strengthen these areas by combining internal expertise with external support, for example, working with a Virtual CISO or consultancy. But before turning to outside help, consider how technology can be a powerful equaliser.

A well-designed platform can ease the load on people, giving them visibility and assurance without the manual burden. It provides a single space to collaborate, track progress, and evidence compliance, freeing specialist resources to focus on higher-value work such as risk strategy and stakeholder engagement.

Crucially, success depends on leadership involvement. Accountability for security can't be outsourced. Senior leaders set the tone, ensuring that information security is treated not as an IT function but as a business-wide discipline.



Remember this

Invest in people first and give them the tools to succeed.

1.3
In considering the technology

Technology underpins every modern business system, and your ISMS should be no exception.

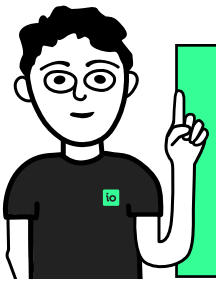
If you wouldn't manage sales, accounting, or HR using only spreadsheets and shared folders, why approach information security that way? The same principle applies: if it's business-critical, it deserves a professional system to match.

An effective ISMS platform brings structure, efficiency, and transparency to the process. It doesn't replace good people or sound governance, it empowers them. It helps teams collaborate, stay audit-ready, and adapt quickly as new risks and regulations emerge.

A good ISMS solution should be:

- **Secure**, meeting independently verified standards.
- **Collaborative**, supporting both internal and external stakeholders.
- **Structured**, ensuring work is joined up and traceable.
- **Flexible and scalable**, adapting as your organisation grows.

Building this technology from scratch rarely makes sense unless software development is your core business. The market already offers mature, affordable solutions that meet these needs, IO among them, giving organisations a faster, more reliable route to implementation.



Remember this

The focus should never be on how to build the technology, but what it enables: Confidence, trust, and control across your organisation.

chapter two

What is an Information Security Management System?

In this section

The components of an ISMS • Why organisations need an ISMS • Is your leadership ready to support an ISMS?

An Information Security Management System (ISMS) is the backbone of an organisation's approach to security and privacy. It connects people, policies, controls, and technology into one coordinated system, ensuring that information is protected, risks are managed, and opportunities for growth are realised.

In simple terms, your ISMS is the nerve centre for how your organisation safeguards and uses information. It governs how data is handled, who has access, and how resilience is maintained.

When well implemented, an ISMS doesn't just prevent harm, it builds trust. It signals to customers, regulators, and partners that your organisation takes security seriously and can be relied upon. And it does so in a way that supports business growth rather than slowing it down.

A strong ISMS can open doors to new contracts, improve supply chain confidence, and streamline compliance with privacy, security, risk and AI regulations worldwide. Conversely, a poorly executed or fragmented system risks undermining business goals and damaging reputation.

Protecting your data is a core part of the picture. Regulations like GDPR place strict demands on how data is managed, but privacy can't exist without security. A well-designed ISMS provides the foundation for both, and more, ensuring compliance while building confidence that the organisation is managing information responsibly.

2.1
The components of an ISMS

An ISMS combines two essential elements:



Both matters.
People drive accountability and culture; the platform provides the structure and consistency that makes good practice repeatable.

Later sections will explore how the balance between these two elements determines not just how well your ISMS works today, but how easily it adapts as the business evolves and optimal return on investment.

2.2
Why organisations need an ISMS

The value of an ISMS is no longer theoretical. It's now a practical necessity, driven by external forces, customer expectations, and regulatory demands.

In an environment where trust is earned, not assumed, an ISMS provides proof. It shows that your organisation has the controls, culture, and oversight required to protect valuable information.

Once, businesses could rely on reputation or informal assurances. Today, they're expected to demonstrate security maturity, whether to regulators, shareholders, insurers, or customers.

A few key drivers explain why:

- **Cybercrime is rising**, costing global economies billions each year and putting every organisation at risk.
- **Regulations are tightening**, with frameworks like GDPR, NIS2, and DORA introducing higher accountability and personal liability for directors.
- **Customers and partners expect assurance**, often demanding evidence of security standards such as ISO 27001, SOC 2 and more recently ISO 42001 for Artificial Intelligence in contracts and tenders.

For many, adopting an ISMS is no longer optional, it's the price of entry for doing business in a connected, data-driven world.

As a result, we're seeing the ISMS become as essential to modern operations as CRMs or accounting platforms. It's the system that protects the organisation's most valuable asset: trust.

2.3

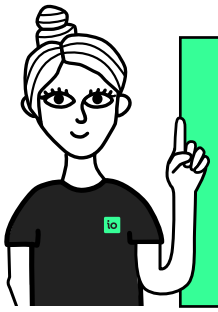
Is your leadership ready to support an ISMS?

Even the best-designed ISMS will struggle without leadership buy-in. Globally governments and industry agencies such as the UK Information Commissioner, The National Cybersecurity Centre and CISA have made it clear: the era of "tick-box security" is over. Security and privacy must be embedded into the fabric of how organisations operate.

We echo that sentiment. Real progress starts when leaders see information security not as a cost or compliance exercise, but as a business enabler that protects value, builds trust, and drives performance. That shift requires clear visibility of risk, confidence that it's being managed effectively, and evidence that investment is delivering results. Treating the ISMS as a strategic business initiative, one that underpins growth, resilience, and reputation, helps create that alignment.

In most organisations, there's already some good practice to build on. Find the people and teams already modelling strong security behaviours and use their momentum to lead wider cultural change.

Finally, decide what success looks like. Is the goal certification to a recognised standard such as ISO 27001, or building trust with key customers and regulators through verified best practice?



Remember this

The answer will depend on your powerful stakeholders, those with the ability to make you act (or regret it if you don't). Their expectations will help shape your ISMS scope, level of assurance, and the investment required.

chapter three

Developing the Business Case for an ISMS

In this section

Benefits to realise • Stakeholder expectations •
Scoping the ISMS to satisfy stakeholder interests • Quantifying the return

No two organisations are identical, but the forces shaping information security are remarkably consistent. Growing cyber threats, evolving regulation, and rising customer expectations have made robust information security a business essential.

Yet, investing in an Information Security Management System (ISMS) isn't just about managing risk, it's about enabling growth. A well-planned ISMS helps organisations protect what matters, operate more efficiently, and prove to stakeholders that they can be trusted.

To build a credible business case, three questions matter most:

What benefits will an ISMS deliver?

Whose expectations must it meet?

How wide should its scope be to deliver lasting value?

3.1

Benefits to realise — achieving returns from threats and opportunities

Security conversations often focus on threats, data breaches, regulatory fines, or reputational damage. Those risks are real, but they're only half the picture.

A mature ISMS also creates opportunity: lower operating costs, better decision making, stronger customer confidence, and competitive advantage.

⚠ Threats highlight what you could lose

Opportunities show what you stand to gain

The table below can help you frame both sides when preparing your business case:

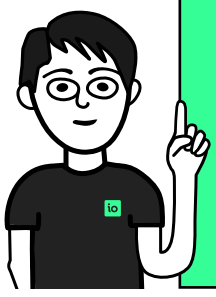
Threats to address

Example threat	Business consideration	Example value measure
Loss of powerful customers who no longer trust your security	What percentage of your customer base demands formal security assurance?	% of customer revenue at risk
Higher cost of sale as customers request repeated security checks	How much time and cost is spent proving trust to each prospect?	£ cost per bid / % sales cost increase
Supplier failures or poor security in your supply chain	What assets or contracts depend on third-party integrity?	£ value at risk / % exposure
Regulatory penalties (e.g. GDPR fines)	What's the financial impact of non-compliance?	£ fine risk / £ legal cost
Reputational damage following a breach	How long would recovery take? What would it cost?	£ PR cost / £ brand loss

Opportunities to unlock

Example opportunity	Business consideration	Example value measure
Growth with existing customers who value your security posture	Can stronger trust support renewals or upselling?	% increase in customer spend
Winning new contracts that require certifications (e.g. ISO 27001)	How many opportunities demand verified security credentials?	£ new business pipeline
Operational efficiency through joined-up risk and compliance	How much time could be saved by consolidating systems?	% process improvement / £ admin savings
Attracting and retaining top talent	Are employees drawn to organisations with modern, responsible security practices?	£ hiring and training savings
Lower insurance costs	Could demonstrable resilience reduce premiums?	% reduction in premium cost

Taken together, these threats and opportunities shape the core return on investment for an ISMS. For many organisations, the question isn't whether the investment pays off, it's how quickly.



Remember this

A well-designed ISMS helps reduce costly incidents, simplify compliance, and unlock growth opportunities. Whether those returns appear as new revenue, cost avoidance, or time savings, the value becomes clear once information security is treated as a strategic enabler rather than a compliance burden.

3.2
Stakeholder expectations — Power, interest, and trust

If the first section does not satisfy the business case for investment, being clear on how well it satisfies the expectations of those who matter most; your stakeholders, is the next step in any business case.

Different groups care about different outcomes:

- **Leaders and shareholders** want assurance that security supports growth and protects value.
- **Customers and partners** need evidence that their data is safe in your hands.
- **Regulators and auditors** expect transparency and proof of compliance.
- **Employees** want to know that their data, and their company, are protected.

The table below outlines typical stakeholder expectations and the level of evidence they may expect:

Stakeholder	Key expectations	Able to evidence now?
Leadership	Confidence that security enables growth, not hinders it; assurance the ISMS is under control; personal risk mitigation	☐
Shareholders	Protection and growth of enterprise value	☐
Regulators & legislators	Proof that privacy and data protection obligations are met (e.g. GDPR, NIS2)	☐
Customers	Visible assurance that the organisation protects their information; trust in supply chain resilience	☐
External auditors	Evidence of compliance with recognised standards such as ISO 27001	☐
Employees	Awareness, training, and confidence in their own role within the ISMS	☐
Suppliers & partners	Trust that your organisation's practices reduce shared risk	☐

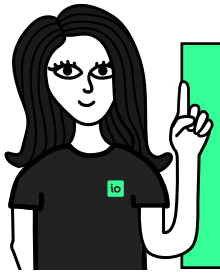
If you are unsure about a stakeholder's expectations from the ISMS, ask them. Ensure that your ISMS is fit for the purpose now, as well as the future.

How much you do in your ISMS and how far you invest depends on which stakeholders you need to satisfy and how valuable the information is to their organisation.

The more visible, auditable, and evidence-based your ISMS becomes, the stronger the trust it creates, both internally and externally. Consider the maturity map below for the more obvious anticipated outputs and outcomes from the ISMS investment (or lack of it).

Maturity Map example

Level	Description	Anticipated Outcome
No compliance framework	Ad hoc or informal security practices	High risk of breach, fines, and loss of trust
Basic compliance (e.g. Cyber Essentials)	Minimum hygiene in place	Limited protection, compliance gaps remain
DIY GDPR compliance	Organisation-defined processes	Reduced risk, but low external assurance
Structured ISMS aligned to ISO 27001	Standardised approach, partially audited	Lower risk and improved customer confidence
Certified ISMS (e.g. ISO 27001)	Independently verified and maintained	High trust, stronger growth, minimal risk exposure



Remember this

Understanding where you are, and where you need to be, helps clarify both the business case and the resources required.

3.3
Scoping the ISMS to satisfy stakeholder interests

An ISMS should always be right sized to your organisation's needs. Its scope depends on what you must protect, who you must satisfy, and how far you want to go beyond minimum compliance.

At a minimum, your ISMS should cover the requirements of major regulations such as GDPR, NIS2, or DORA, depending on your sector. But forward-thinking organisations take it further, adopting internationally recognised frameworks like ISO 27001 and SOC 2 for information security and ISO 42001 for artificial intelligence to build resilience, consistency, and trust across their operations.

3.3.1 GDPR-focused work

Following a regulation such as GDPR alone will mean doing the work listed below:

- Mapping and classifying personal data
- Conducting risk assessments and DPIAs
- Managing subject access requests and consent
- Implementing staff training and awareness programmes
- Demonstrating accountability through documented policies and audits

This approach meets immediate privacy obligations but may not address wider security or operational risks.

3.3.2 Broader security and assurance

Extending the ISMS beyond GDPR to frameworks like ISO 27001 for information security and ISO 42001 for AI delivers higher ROI and future-proofs compliance. It creates a unified system that manages all valuable information assets, from intellectual property and financial data to supplier and operational information.

Organisations following this path typically see:

- Greater alignment between risk management and business strategy
- Easier adoption of new regulatory requirements
- Stronger trust from customers, partners, and auditors

3.3.3 Work required for ISO 27001

ISO 27001 may seem complex at first glance, but it's a logical, business-led framework built around continuous improvement. It requires organisations to:

- Understand internal and external context
- Define scope and objectives
- Identify and treat information security risks
- Establish roles, responsibilities, and policies
- Measure and improve performance over time

While there's detailed work involved, much of it overlaps with regulatory requirements businesses are already required to comply with. For most organisations, building the foundation of their ISMS on ISO 27001 is a practical approach to meet these varying regulations more efficiently and turn compliance into a strategic capability.

ISO 27001 Annex A Controls

Organisational Controls (A.5.1–A.5.37)

Identifier	Annex A name
A.5.1	Policies for information security
A.5.2	Information security roles and responsibilities
A.5.3	Segregation of duties
A.5.4	Management responsibilities
A.5.5	Contact with authorities
A.5.6	Contact with special interest groups
A.5.7	Threat intelligence
A.5.8	Information security in project management

Identifier	Annex A name
A.5.9	Inventory of information and other associated assets
A.5.10	Acceptable use of information and other associated assets
A.5.11	Return of assets
A.5.12	Classification of information
A.5.13	Labelling of information
A.5.14	Information transfer
A.5.15	Access control
A.5.16	Identity management

Identifier	Annex A name
A.5.17	Authentication information
A.5.18	Access rights
A.5.19	Information security in supplier relationships
A.5.20	Addressing information security within supplier agreements
A.5.21	Managing information security in the ICT supply chain
A.5.22	Monitoring, review and change management of supplier services
A.5.23	Information security for use of cloud services
A.5.24	Information security incident management planning and preparation
A.5.25	Assessment and decision on information security events
A.5.26	Response to information security incidents
A.5.27	Learning from information security incidents

Identifier	Annex A name
A.5.28	Collection of evidence
A.5.29	Information security during disruption
A.5.30	ICT readiness for business continuity
A.5.31	Identification of legal, statutory, regulatory and contractual requirements
A.5.32	Intellectual property rights
A.5.33	Protection of records
A.5.34	Privacy and protection of personally identifiable information (PII)
A.5.35	Independent review of information security
A.5.36	Compliance with policies and standards for information security
A.5.37	Documented operating procedures

People Controls (A.6.1–A.6.8)

Identifier	Annex A name
A.6.1	Screening
A.6.2	Terms and conditions of employment
A.6.3	Information security awareness, education and training
A.6.4	Disciplinary process

Identifier	Annex A name
A.6.5	Responsibilities after termination or change of employment
A.6.6	Confidentiality or non-disclosure agreements
A.6.7	Remote working
A.6.8	Information security event reporting

Technological Controls (A.7.1–A.7.14)

Identifier	Annex A name
A.7.1	Physical security perimeter
A.7.2	Physical entry controls
A.7.3	Securing offices, rooms and facilities
A.7.4	Physical security monitoring
A.7.5	Protecting against physical and environmental threats
A.7.6	Working in secure areas
A.7.7	Clear desk and clear screen

Identifier	Annex A name
A.7.8	Equipment siting and protection
A.7.9	Security of assets off-premises
A.7.10	Storage media
A.7.11	Supporting utilities
A.7.12	Cabling security
A.7.13	Equipment maintenance
A.7.14	Secure disposal or re-use of equipment

Platforms like IO simplify this journey, offering structured templates, guidance, and automation to help organisations adopt, adapt, and add to their ISMS with confidence and clarity.

A well-scoped ISMS is not about over-engineering, it's about matching investment to value at risk.

The right approach should meet today's expectations, prepare for tomorrows, and deliver a return that justifies itself many times over.

To complete your business case, the next step is to quantify that return, demonstrating the tangible and measurable value of investing in your ISMS.

Free download

To find out more about the journey to ISO 27001 certification, download our free guide

Get your guide →



3.4

Quantifying the return — calculating ROI and telling the value story

When it comes to information security, proving return on investment can feel challenging. Unlike revenue or sales metrics, the benefits of an ISMS are often seen in what doesn't happen, the breaches avoided, the fines prevented, the customers retained.

But those "non-events" have very real financial value. A single data breach can cost millions in direct losses, reputational harm, and recovery effort. A well-planned ISMS turns that potential loss into a measurable saving, and beyond that, it delivers new commercial opportunities and operational efficiencies that strengthen the business overall.

3.4.1 A structured approach to ROI

Calculating ROI for your ISMS starts with three clear steps:

1. **Identify the benefits** — both tangible (cost savings, new revenue, reduced risk) and intangible (trust, reputation, culture).
2. **Quantify the investment** — including technology, people, training, and maintenance.
3. **Compare the value** — using a consistent timescale, typically three to five years.

The simple formula below helps to visualise that comparison:

ISMS ROI =
(Total Value of Benefits – Total Cost of Ownership)
÷ Total Cost of Ownership

If the result is positive, the ISMS is paying for itself, often many times over.

But numbers alone rarely make the case. The story behind them matters just as much as how the ISMS aligns with business goals, reduces uncertainty, and enables future growth.

3.4.2 Typical benefits to quantify

1. Risk Reduction and Cost Avoidance

- Reduced likelihood of data breaches or cyber incidents
- Lower potential penalties from non-compliance (e.g., GDPR fines)
- Less downtime and disruption from security events
- Reduced insurance premiums through demonstrable risk maturity

2. Efficiency and Operational Savings

- Streamlined processes for audit and evidence gathering
- Fewer manual tasks and duplicated systems
- Better visibility across departments for faster decision-making
- Simplified reporting and stakeholder communication
- Better decision making through systematic data processing

3. Growth and Opportunity

- Ability to bid for contracts requiring ISO 27001 certification
- Faster capability to comply with emerging regulations and achieve compliance with other frameworks such as ISO 27701 for privacy, ISO 42001 for AI and SOC 2 in the US
- Improved customer retention and trust
- Increased partner and supply chain confidence
- Stronger brand reputation and competitive differentiation

Each of these categories contributes to both direct and indirect ROI, from saving time and money to opening doors that were previously closed.

3.4.3 Typical costs to include

Cost Category	Example Inclusions	Notes
People	Project management, training, awareness programmes	Upfront and ongoing
Technology	Platform or tool subscriptions, integrations	Scalable, predictable cost
External Expertise	Consultants, auditors, certification fees	Varies by scope and support
Maintenance and Improvement	Internal reviews, control testing, updates	Continuous improvement built in

While there are clear financial costs, the most significant "expense" is often time, especially when trying to build or maintain an ISMS manually. Automating repetitive tasks and consolidating documentation can dramatically reduce this burden.

That's where platforms like IO add value. They provide a ready-made foundation, templates, and workflows that shorten implementation time and reduce long-term maintenance costs, making the return on investment faster and more sustainable.

3.4.4 Demonstrating the value story

When presenting your ISMS business case to leadership or the board, focus on three principles:

1. Link security to strategy.

Position your ISMS as an enabler of business growth, customer trust, and resilience, not just compliance.

2. Show the numbers but tell the story.

Combine financial data with relatable business scenarios: "If this control prevents one serious incident per year, it pays for itself."

3. Highlight the momentum.

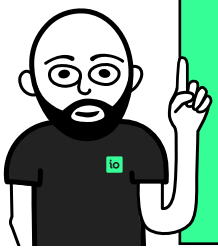
Emphasise that an ISMS isn't a static project, it's a living system that matures with the business and continually delivers value.

Boards respond to clarity and confidence. Show them that investing in an ISMS is not about avoiding failure, it's about building a stronger, more trusted, more competitive organisation.

3.4.5 Summary: Turning ROI into long-term value

The ROI of an ISMS isn't just about the first year's numbers; it's about sustained advantage.

Over time, the organisations that invest in structured information security consistently outperform those that don't. They win more business, recover faster from disruption, and maintain stronger relationships with customers, regulators, and investors.



Remember this

In short, the ISMS pays for itself many times over, financially, operationally, and reputationally.

With a clear business case in hand, the next logical step is deciding how to make it happen, whether to build your ISMS internally or adopt a proven platform that accelerates and sustains success.

chapter four

Build or buy? Considering the best way to achieve ISMS success

In this section

Understanding what's involved in an ISMS solution • What to look for in an ISMS technology solution • Evaluating total cost of ownership (TCO) • Long-term value and maturity • The balance of people and platform

Once you've built the business case for an ISMS, the next question is how to make it happen.

Broadly, there are two options:

- **Build your own ISMS internally**, designing the framework, processes, and tools from the ground up.
- **Buy a proven platform or solution** that accelerates implementation and simplifies ongoing management.

Both approaches can work, but the right one depends on your organisation's size, complexity, and needs. Whichever path you take, it's essential to view your ISMS as a long-term investment, not a one-time project. The goal isn't just to get certified, it's to embed information security, privacy, and resilience into how your organisation operates every day.

4.1

Understanding what's involved in an ISMS solution

An effective ISMS combines two core elements, people and technology, both of which must work together to deliver sustained results.

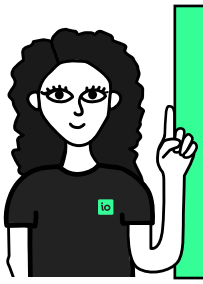
While content such as policies, procedures, and controls is vital, they're only one part of the equation. The way your ISMS is designed, coordinated, and maintained will determine whether it becomes a living system or another static compliance exercise.

Common pitfalls include:

- Buying cheap, generic policy templates that aren't aligned to your organisation's realities.
- Over-relying on consultants who don't share their methodology, leaving you dependent on them long-term.
- Building folder-based systems that store documents but fail to provide visibility, reporting, or coordination.

These shortcuts may appear cost-effective initially but often become resource-heavy and inconsistent over time. Manual tracking, version control issues, and duplication of effort can make audits painful and ongoing maintenance inefficient.

A self-built ISMS also relies heavily on the individuals who designed it. If they leave the organisation, so does the knowledge, making continuity and improvement difficult. For many organisations, these risks outweigh the perceived benefits of control.



Remember this

A sustainable ISMS needs to balance effort and investment with ongoing value, integrating security and compliance into daily operations, not bolting it on once a year.

4.2
What to look for in an ISMS technology solution

Technology should sit at the heart of your ISMS, not as a replacement for people, but as the structure that supports them.

A good ISMS platform provides:

- **Preconfigured best practice frameworks** aligned to recognised standards such as ISO 27001.
- **Structured guidance and templates** that reduce guesswork and manual effort.
- **Integrated workflows and automation** to manage risk, documentation, and compliance activities in one place.
- **Real-time reporting and dashboards** to track progress and demonstrate control to auditors and leadership.
- **Built-in collaboration tools** for both internal teams and external auditors.

Together, these capabilities support the following core characteristics of a good ISMS technology solution:

Characteristic	Description
All-in-one-place	A centralised location for all ISMS-related activities and documentation, eliminating the need for messy spreadsheets.
Security for management software	The software used to manage the ISMS must itself be secure to protect the information it holds.
Always Accessible	Users can access the ISMS and its information from anywhere, as long as they have the necessary authorisation.
Easy to use	Designed to be intuitive and user-friendly, often with built-in guidance to simplify the process for users, especially beginners.
Structured for success	Provides a clear, structured path to achieve compliance, often following established standards like ISO 27001.
Joined up	All parts of the system work together seamlessly, with integrations and automated workflows connecting different components.
Transparent	The system is clear and open, allowing for easy visibility into security activities and status across the organisation.
Collaborative	Facilitates teamwork and collaboration among different roles and departments involved in information security.
Insightful & actionable	Provides clear insights and actionable data that help users understand risks and make informed decisions.
Affordable	Offers a cost-effective solution, which might be a low, predictable cost over time instead of a large upfront investment.

For most organisations, this approach offers the best balance of speed, assurance, and cost-effectiveness.

It allows your people to focus on strategy, awareness, and improvement, the parts of information security that technology alone can't do, while the platform takes care of structure, visibility, and evidence.

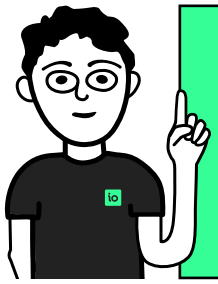
Platforms like IO go one step further.

They're designed specifically to deliver compliance success, bringing together years of domain expertise, integrations, and proven processes that remove the uncertainty from ISMS implementation. The result is faster certification, easier maintenance, and consistent results year after year.

4.3
Evaluating total cost of ownership (TCO)

When comparing build vs buy, it's tempting to focus on upfront cost. But the real measure is total cost of ownership, how much it costs to achieve, maintain, and evidence compliance over time.

Cost Factor	Build Internally	Buy a Proven Platform
Initial setup	Lower direct spend, higher internal labour	Predictable subscription, minimal setup effort
Expertise required	High – depends on internal capability	Prebuilt expertise and structured guidance included
Implementation time	6–12 months on average	Often 50–70% faster
Audit readiness	Manual evidence gathering	Continuous audit readiness built in
Maintenance	Ongoing manual effort	Automated updates and tracking
Scalability	Limited by internal systems	Built to scale with growth
Risk of failure	Higher – process dependent on individuals	Lower – proven, repeatable approach



Remember this

The most efficient ISMS implementations combine people and platform intelligently: people define the priorities and culture; the platform provides the discipline, visibility, and automation to deliver lasting value.

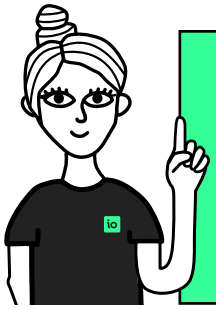
4.4
Long-term value and maturity

Building or buying is not just a one-off decision, it's a commitment to continuous improvement.

An ISMS should evolve alongside your organisation, adapting to new risks, regulations, and business opportunities. That means the system you choose needs to support ongoing learning, adaptation, and scalability.

With a homegrown ISMS, continuous improvement often becomes reactive, dependent on individual effort or external audits to trigger updates.

With a structured, platform-based approach, improvement is built in. You gain visibility across policies, risks, and controls, can benchmark progress, and act proactively when issues arise.



Remember this

In the long run, this visibility translates directly into business resilience. It enables better decisions, faster responses, and stronger trust across your ecosystem, all while reducing the overhead of staying compliant.

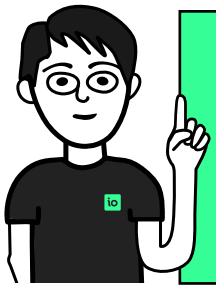
4.5
The balance of people and platform

The real question isn't build or buy, it's how do we use our people best?

Technology should take care of the structure and routine so that your people can focus on what only humans can do:

- Making informed risk decisions.
- Engaging teams and embedding culture.
- Communicating security value to customers, partners, and boards.

When people and technology work together, information security becomes easier to manage, more consistent, and ultimately more valuable.



Remember this

That's where IO's approach excels by integrating intuitive technology with expert guidance, it helps organisations achieve compliance faster, maintain it more easily, and build the confidence to scale securely.

chapter five

Why IO?

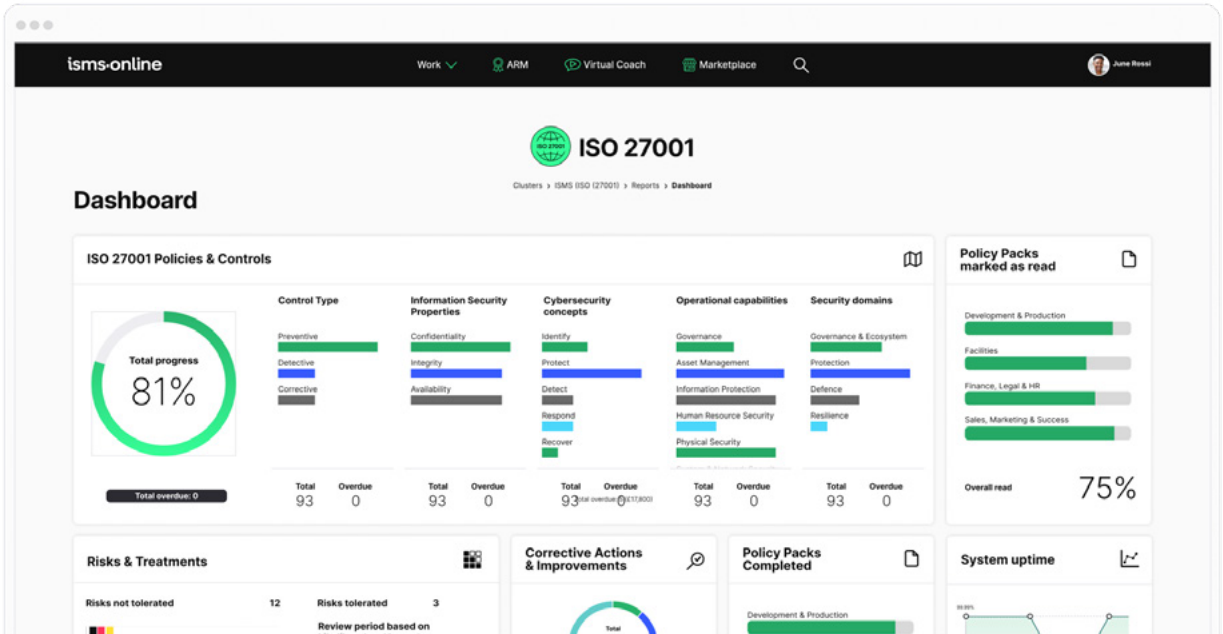
In this section

What makes IO different • The IO advantage •
Trusted by auditors and customers alike • Partnering for the long term

By now, the case for an Information Security Management System is clear. It protects what matters, builds trust with stakeholders, and strengthens your organisation for the long term. But building and maintaining one shouldn't be harder than the security challenges it's designed to solve.

That's where IO comes in.

IO brings together everything organisations need to implement, maintain, and continually improve their ISMS, all in one secure, purpose-built platform. It combines deep domain expertise with intuitive technology to make compliance straightforward, sustainable, and scalable.



5.1
What makes IO different

Proven Success

Over 25,000 users worldwide rely on IO to achieve and maintain compliance with confidence.

From growing businesses to global enterprises, IO helps organisations reach certification on their first attempt and stay audit-ready thereafter.

Built on Best Practice

IO is preconfigured with recognised frameworks such as ISO 27001, ISO 27701, and SOC 2, so you can start from a position of strength. Our Assured Results Method guides teams' step by step through the process, giving structure, clarity, and confidence from day one.

Designed for People

Security and compliance succeed when people engage with them. IO's platform is built for collaboration, not complexity, making it easy for teams to understand their roles, evidence their work, and maintain momentum.

Sustainable by Design

Unlike static systems or consultant-led projects, IO grows with your organisation. It provides ongoing visibility, benchmarking, and guidance to keep your ISMS aligned with evolving risks, regulations, and business priorities.

5.2
The IO advantage

Advantage	What It Means for You
Speed to Success	Achieve certification faster with prebuilt frameworks and guided workflows.
Sustained Compliance	Stay audit-ready all year round with automated updates and continuous monitoring.
Scalability	Expand effortlessly across frameworks and regions as your organisation grows.
Confidence and Trust	Demonstrate compliance to customers, partners, and regulators with ease.
Reduced Cost and Complexity	Eliminate duplicated effort and manual admin through automation and integration.

5.3
Trusted by auditors and customers alike

Auditors worldwide recognise IO as a trusted platform that delivers complete, consistent, and transparent ISMS management.

Our customers, from fintechs and SaaS providers to healthcare and professional services, repeatedly achieve certification success, operational efficiencies, and measurable ROI through IO.

They value the simplicity, reliability, and long-term partnership we provide.

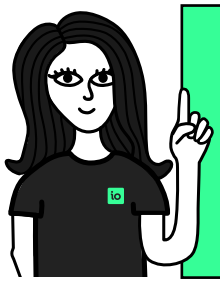
NHS Professionals · ScottishPower · FLIGHT CENTRE · SIEMENS · TUI · rightmove · Panasonic · moneycorp · BDO

5.4
Partnering for the long term

Implementing an ISMS is not a one-time exercise; it's a commitment to continual improvement. IO's mission is to make that commitment achievable, practical, and rewarding.

By blending human expertise with intelligent technology, we help organisations move beyond compliance towards resilience, growth, and lasting trust.

In a world where trust defines success, IO helps you earn it and keep it.



Remember this

Whether you're starting from scratch, upgrading existing processes, or aligning multiple frameworks under one roof, IO provides the structure, support, and assurance you need to succeed.

About io

At IO, we believe compliance should fuel progress, not hold it back.

That's why we built a modern platform to simplify, strengthen, and scale information security, privacy, risk and AI management. Supporting 100+ global standards, including ISO 27001, ISO 27701, ISO 42001, GDPR, and NIS 2, IO gives teams everything they need to stay secure, aligned, and audit-ready in one place.

Our approach blends people, process, and platform, because lasting compliance isn't achieved by automation alone. With guided support, structured workflows, and smart integrations, IO embeds compliance into daily operations—reducing duplication, surfacing insights, and building confidence.

Trusted by thousands worldwide, IO turns compliance from a box-ticking chore into a strategic advantage.

Explore more at isms.online