isms.online

Planning the business case for an

Information Security Management System

For organisations that are serious about their information security

PUBLIC | V2.0

Contents

An ISMS delivers a positive return on investment. The goal of this paper is to show you why, what, and how you can get RoI from an ISMS that fits the business needs.

Unsure where the value is? Looking for a more strategic and pragmatic approach to information security? This paper sets out the main issues behind planning the business case for an information security management system (ISMS).

It is written with two audiences in mind:

1. Those relatively new to information security with a basic understanding of the terminology and landscape already but unsure where the value is from an ISMS.
2. Information security improvers and experts who are struggling to get traction with their efforts to secure funding for more strategic and serious solutions like an ISMS.

Information security is complicated as it touches every part of the organisation and means different things to different people.

However, it does not need to be as hard or as expensive as many suggest. The right people combined with the right technology makes it much more accessible and affordable to do well.


isms.online
Home
Work
ARM
Virtual Coach
ISMS
Work areas
Updates
Reports
Discussions
Documents
To-dos
Project Activities
Track Items
To-dos
Team
Settings
Dashboard
Risks & Treatments
Risks not tolerated
Treat (Other)
Transfer
Terminate
Combination of actions
Not specified
Risks tolerated
Tolerate
Review period based on Likelihood and Impact
Review overdue 1
Security Incident Management
Total 3
Overdue 2
Corrective Actions & Improvements
Total 7 £17,800
Overdue 3 £17,800

About ISMS.online

ISMS.online is powerful cloud software that helps deliver an information security and privacy management system that stakeholders can trust, at a fraction of the cost, time and risk of alternatives.

ISMS.online is ideal for organisations that are serious about information security, yet don't have the budget and resources for some of the very expensive solutions and hard to use services in the market. It makes the people side of the ISMS equation much easier and more sustainable to solve too whether that is from internal or external sources.

Specialist infosec & privacy partners offer Virtual CISO, DPO and related services both inside and alongside ISMS.online.

ISMS.online also has complementary resources such as Virtual Coach, and actionable policies and controls built in to quickly adopt, adapt and add to.

01

Executive Summary

Cybercrime and information loss is one of the most significant threats to nation states, business and society today

Internationally the cost is many tens of billions of pounds, and consequences from poor security practices can be life affecting let alone business changing. Regulatory pressures for stronger privacy practices are growing too.

The introduction of the new General Data Protection Regulations (GDPR) and a host of other national regulations has further increased the burden on organisations to protect personal and other data.

With overwhelming evidence being presented about the threats, many organisations still fail to take adequate steps to prevent harm against themselves, their customers or the supply chain.

Certified standards such as ISO 27001:2013 and basic cyber hygiene e.g. from Cyber Essentials are becoming more popular but they are not yet mainstream.

Why is that?

1.1 Three reasons why nothing happens

REASON 1:
Not having a compelling internal need to act

Aside from more forward-thinking leaders who are prepared to invest, it's not seen as a priority for many leaders right now. Whilst the evidence of threat is overwhelming, until a loss happens to them or someone they know, nothing material happens beyond operational security purchases e.g. antivirus, firewalls, etc.

Depending on your starting point and stakeholder expectations for the future, doing nothing is not an option any longer. External forces for change are mounting and need to be considered carefully as do external stakeholder expectations.

Regulations are directing organisations towards more professional approaches to security and protection. One simple data breach can kill a company and could have devastating consequences for the stakeholders who suffer loss. Powerful customers are also getting smarter about managing their supply chain risks and mitigating against failure. However, whilst forces pushing for change are high, unless resisting forces are addressed, any ISMS implementation is unlikely to be successful or sustainable.

REASON 2:
People not knowing what to do or how best to do it

There is so much noise in the info sec and privacy world right now. So much choice yet with little clarity on the benefit, people just don't act because they can't be sure they are making the right decisions. They may not have the time, interest or expertise for learning about the subject either.

Looking at the needs of powerful stakeholders is crucial. In the absence of clearer direction from powerful customers, or regulators on what a certification standard looks like for GDPR, following minimum standards such as ICO checklists, Cyber Essentials, and for more comprehensive approaches, ISO 27001:2013 is a good way forward.

We present the information security maturity map later and assess stakeholder expectations to help determine a minimum foundation for your organisation and plan future goals it might want to move towards.

There are also some companies with very deep pockets for marketing and sales, drawing lots of fanfare.

Their product investments and user experience may not have had the same care and attention. The information security management sector for both physical support offerings and technology continues to evolve too.

As such we urge organisations to look beyond the marketing hype to ensure vendors deliver on their promise and demonstrate they can be trusted too.

REASON 3:
Seeing infosec and privacy purely as a cost

Information security and privacy management can be a struggle for some leaders to get excited about, so they only see one part of the equation; cost. They also consider it as very complicated so without addressing reasons 1 & 2 it remains in the 'too hard box'.

Moving resistant people internally from a cost to benefit mindset is crucial for success and leadership buy in.

More strategic and professional information security management needs to show the return part of the equation and be considered an investment, not just a cost.

The RoI can be compelling when done with serious consideration. It also needs to recognise that like professional sales, accounting and other key business systems, an ISMS needs more than a shared folder store, emails, spreadsheets and documents to make it work well.

Aside from the cyber criminals involved in this area, there really can be business winners, not just losers or more costs to budget for in future.

For those who take the topic seriously, the RoI from better information security and privacy can be very attractive too but it takes a strategic approach to the subject. Whether that is a real return on the bottom line, future cost avoidance or better risk management is something this paper can help you consider.

The paper sets out to help determine the RoI and includes the following aspects which you can build on for your own organisation's business case:

What an ISMS is and how the combination of people and technology that deliver it are crucial for achieving an optimal RoI. The people and technology can come from internal sources or be complemented by external resources too.

Why you should have an ISMS. If you or your leadership don't already believe then this will help you determine where the benefits can materialise, including:

- Financial and reputational threats, areas for future cost avoidance.
- Opportunities for growth and material gain.

Who the stakeholders are and what their expectations might include. That will help form your ISMS scope and consider how far to go with the solution, ranging from basic GDPR, into cyber hygiene through to more comprehensive standards-based methodologies like ISO 27001:2013.

To build or buy, and whether to use your own people, complement them with external resources and how to evaluate the technology component of the ISMS.

The equation for RoI from an ISMS is simply as follows:

Forces driving for change + **Powerful stakeholder expectations** + **Benefits from the ISMS**

LESS

Resisting forces + **Costs of people & technology for the ISMS during implementation and ongoing management**

As with any business case analysis, increasing the numerator is great, and decreasing the denominator is also likely to be of value in reducing risk, cost and time to get work done.

Depending on your value at risk and the size of the opportunity or threat, the document may lead towards an immediate decision to do something, or perhaps involve much more planning and analysis before decisions are taken.

Whatever the size enterprise, the return will almost certainly outweigh the investment of people and technology, assuming the resisting forces can be addressed.

1.2 A point on people

In considering the people have in mind the following:

3 Cs: Capacity, Capability and Confidence.

The people involved need the capacity to get the work done, the capability to perform the jobs and the confidence to know what to do.

External support can be great to help with any of the 3 Cs but before choosing a third party also consider the use of technology to ensure you have visibility, transparency, sustainability and lowest total cost of operation. Good technology helps with capacity, capability and confidence too, freeing up any specialist resources to focus on the thorny and specific needs of the organisation.

Ensure your leadership is involved. Do not abdicate accountability and select a firm or people that take a business led strategic approach to security, who follow recognised standards and are experienced in working in a digital paperless fashion.

1.3 In considering the technology

If you run your sales, accounting and other key business systems using excel sheets and word docs, relying on emails and folders for sharing, then you'll probably want to do the same here.

If you are however serious about information security and privacy, you'll want to show that too with a professional platform in the same way that Salesforce.com, Xero etc deliver for their target audience.

Sheets, docs, emails have a role in the ISMS like they do in sales and accounting solutions, but they are not the only thing you need for success.

A good ISMS solution meets the 10 characteristics described later and covers the scope of ISMS to meet the stakeholder expectations now and in the future.

You can build or buy the technology but stick to your core competences. If you wouldn't build Salesforce.com don't build the technology for your ISMS, there are better options out there already. Ensure your focus is on what you are trying to achieve with the ISMS, not worrying about how to do it.

02

What is an ISMS?

An Information Security Management System (ISMS) describes and demonstrates an organisation's approach to Information Security (and privacy management).

It includes how people, policies, controls and systems identify, then address the opportunities and threats revolving around valuable information and related assets.

Put simply an ISMS is the nerve centre, the holistic point of coordination and control behind the strategic and operational work done to protect and harness valuable information.

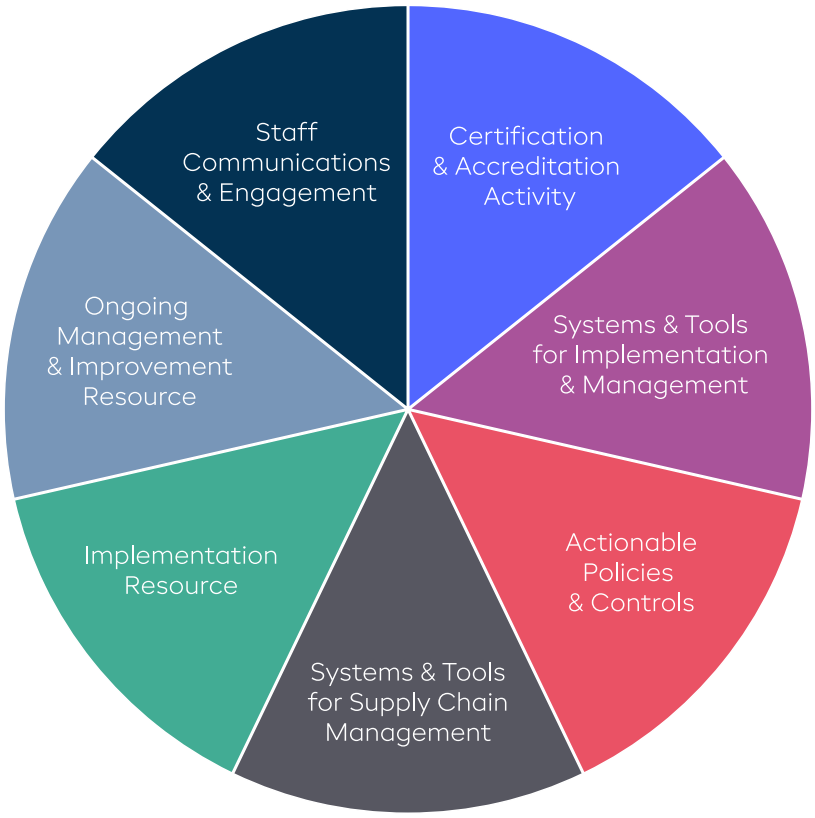
A good 'joined up' professional ISMS shows stakeholders the organisation can be trusted and is serious about its approach to security. Implemented well and with a business led approach to security, organisations can generate attractive returns on their investment from an ISMS.

These include positive growth factors such as helping to win new business as well as mitigating increasing risks in areas such as cyber-crime and privacy regulation.

On the other hand, a poor ISMS lacking the ability to win confidence, nor help improve practices, will undermine the wider organisation goals. A poor ISMS could bring about bigger risks and losses than it was intended to address.

Privacy is a big topic with regulations like GDPR being front and centre right now. Privacy is not achieved without security therefore a well configured ISMS can help achieve trust in both areas, whereas a privacy management system is generally more limited in its scope.

2.1 What are the components of an ISMS?



An ISMS will have two broad investments behind it:

1. People

2. Technology

Later in the paper we look in more depth at the people and the technology behind ISMS success, and the mix of both you should consider for sustainable success and optimal return on investment.

Before that, it is essential to understand ‘why’ an ISMS is becoming much more important.

If you believe, no proof is necessary.

If you don't believe, no proof is possible.

2.2 Why do organisations need an ISMS?

Whilst the return on investment from an ISMS can be high as we illustrate later, triggers for the initial investment generally come from external forces such as powerful customers.

Forward thinking internal leaders are starting to believe in the benefits of an ISMS too, however until recently, little effort has gone into demonstrating the business case for an ISMS.

There are also growing numbers of other stakeholders much more interested in how their valuable information is used and protected. And as pain from failure is increasing, organisations need better ways of demonstrating they can be trusted to those stakeholder groups.

Any historical belief about organisations naturally protecting privacy and security of valuable information is quickly being eroded towards a default of disbelief and distrust. The burden of proving an organisation can be trusted is therefore growing rapidly. A good ISMS helps address those issues.

Cyber-crime is one of the fastest growing issues facing society, costing billions of pounds to economies and destroying lives. Privacy issues are growing rapidly too. Facebook and Cambridge Analytica are current examples for destroying belief and trust for millions of users but there are plenty of others especially at a business level; just look at the fines and activity increasingly being reported by the Information Commissioner's office.

Cyber-crime is one of the fastest growing issues facing society, costing billions of pounds to economies and destroying lives.

It is why regulations like GDPR are being implemented to protect vulnerable individuals against powerful or untrustworthy organisations. Of course, corporate buyers are getting much smarter too, not just because of the personal data issues, they have other valuable information assets in their organisation too.

That is why standards and certifications such as ISO 27001:2013 are increasingly being requested by powerful customers. A good ISMS makes those standards much easier to achieve and sustain as well.

As an example of the changing times, the UK Government has recently added in G-Cloud 10 contract call off terms that (if requested by the buyer) suppliers will have an ISMS. Realistically if a supplier wants to win business in the future they will already have an ISMS in place.

They'll also have one that their customer can trust quickly and easily, visibly and transparently. Otherwise it will increase barriers and costs of sale and might well result in the buyer going elsewhere.

It's not just government contracts either. Data Protection Officers (DPO's) and Chief Information Security Officers (CISO's) across private, public and third sector organisations are now starting to push requirements for demonstrating information security credentials into their supply chain too.

Some customers are being responsible about that change, helping suppliers build capability, whereas others are simply forcing contract changes about privacy and security risk transfer. Either way, the supply chain needs to invest in this area and develop an ISMS that can be trusted. For more information in the ISMS.online Responsible Customer Programme, visit the website.

Boards and shareholders are also becoming much more aware of their own personal exposure, both reputationally and financially too. With growing demands for personal consequences on company directors, we see legislation driving investment towards proactive protection with ISMS, beyond blunt insurance policy instruments.

Indeed, switched on insurers will reward (or probably not penalise) those customers who can demonstrate a good security posture.

Some of the actuary models for deriving premiums are pretty basic and many of the insurers remain clueless despite this being one of the fastest growing sectors.

That will also change very quickly too, reinforcing why an ISMS with all its broader benefits makes sense rather than just taking on higher premiums.

Hope is not a strategy for information security, and sales rhetoric with basic ‘trust me’ policy statements are simply not going to work any longer. It might take another year or two, but the expectations are growing. We will see ubiquity in business for professional ISMS solutions in the same way we do now with customer relationship management systems like salesforce.com and accounting systems like Xero.

The amount of work for a business case is dependent on how much the organisation already believes in the need for the ISMS and how ready the leadership are to embrace it.

2.3 Is your organisation leadership ready to support an ISMS?

The Information Commissioner for the UK Supervisory Authority leading on GDPR is on a mission to move UK PLC away from 'tick box' security and privacy to embedding it into the fabric of organisations.

We echo that vision. Regardless of the business case benefits in theory, if leadership don't believe in security and privacy benefits themselves, it's unlikely to be a success in practice.

More visibility in the business case benefits and treating an ISMS like any other investment is a great way to help bring leadership onside, and this document will help with that planning.

It's also likely there are already pockets of good information security and privacy practice, tacit or explicit. It's unusual to be starting from zero so finding the hero leaders with good habits is a sensible place to build on and get them to model the new behaviours for all.

The organisation also needs to decide the specific outputs from investing in an ISMS e.g. whether to get an independent certification for a recognised standard like ISO 27001 from a body like UKAS.

To a large degree that may be driven by the external forces such as your powerful stakeholders* expectations, competitor points of differentiation and the requirements of being in the market and the value at risk from your current ways of working. These are all considered in more depth as part of developing the business case for an ISMS.

* We describe powerful stakeholders as the ones with the ability (alone or collectively) to make you act (or regret it if you don't).

ISO 27001 is one of the most sought-after information security standards in the world, with certifications growing by more than 450% in the past ten years.

It is globally recognised as the benchmark for good security practice and supports compliance with a host of laws, including the EU's GDPR regulations.

03

Developing the business case for an ISMS

One size doesn't fit all when it comes to delivering an ISMS.

Beyond the forces driving for or resisting change, four factors will affect how to approach the ISMS and each one has a role in the business case considerations.

Benefits to realise
Achieving returns from the threats and opportunities

Stakeholder expectations for the ISMS given their relative power and interest

Scoping the ISMS to satisfy stakeholder interest

Build or buy
Considering the best way to achieve ISMS success

3.1 Benefits to realise - Achieving returns from the threats and opportunities

The most popular information asset being talked about at the moment is personal data, with new privacy regulation such as GDPR driving that focus.

There are however many other types of information asset that organisations should be considering within their ISMS as the benefits from protecting and harnessing them may be significant too.

As we know, organisations increasingly have to show they can be trusted for information security and privacy management.

If they can't and competitors or substitutes can, the organisation's future is at risk. With increased regulation and powerful customers getting smarter every day it may no longer be about standing out from the crowd with an ISMS either.

That might just be a minimum entry to a tender, a contract renewal or an attractive market opportunity.

Whilst the minimum information asset that needs to be protected is personal data to meet the GDPR, consider the other valuable information assets for your ISMS scope too, especially if you have powerful stakeholders who expect other information assets to be protected as well.

An information asset is simply defined as “anything information based that has value to the organisation”.

Information asset	Relevance to your organisation?
Personal data e.g. customers, staff, others	
Intellectual Property e.g. source code, patents, designs, thought leadership etc	
Financial and commercial information; plans, contracts, processes and procedures	
Customers, suppliers and other important relationship information assets (beyond personal data)	
Networks, hardware and other information processing facilities	
People with key knowledge that affect business performance	
Other?	

Information security is not all stick, there are carrots too. Whilst there are lots of sensible ‘threat’ based reasons to invest in an ISMS there are many* positive growth ‘opportunities’ and benefits for having an ISMS too.

The threats and opportunities outlined below will trigger areas of investigation to help the business case ‘returns’ and justification for an ISMS.

* Rather than look specifically at tactical, operational security threats e.g. from malware, or a door left unlocked, this work is deliberately more strategic in its business case focus.

Threats	Considerations for your business case	Value / measure example	Your estimate
Existing (especially powerful) customers no longer believe you can be trusted so avoid renewing your contracts	What percentage and financial value of your customer base is powerful enough to demand an ISMS (e.g. independently certified or at least more visible than what you have now?)	% of customers powerful enough to force change. £ contract value of powerful customers. £ contract value of all customers.	
Cost of sale increases as more prospects seek assurances from information security and privacy practices	How much more will your selling costs increase to demonstrate you can be trusted? (e.g. extra sales hoops to jump through, more paperwork and audits to undertake)	% increase in cost. £ increase in direct cost of sale per opportunity. £ indirect increase in total cost from receiving fewer opportunities to bid on.	
Go-to-market partners no longer believe you can be trusted so avoid promoting and reselling your products and services	What percentage and financial value of your channel to market is powerful enough to demand an ISMS they can trust?	% of channel partners. £ partner revenues.	
Your important suppliers are poorly managed by you or unable to demonstrate they can be trusted and you face consequences from their performance failures	What are the threats by suppliers not performing or breaching confidentiality, integrity or availability of information?	£ value of assets managed or accessible by suppliers. % and £ of customer contracts likely to be lost.	
Powerful suppliers actually consider you too big a GDPR risk to process personal data for, or increase prices to reflect their risk appetite on supply	What percentage of your data processors may consider your approach to GDPR a risk for them given regulation change?	£ supply side price increases for risk. % of business at threat of non-supply/ no alternatives.	
Loss of valuable information from a breach affecting future trading capability: financial, personal, IPR, contracts etc	Consider the type and value of your organisation's information assets and if appropriate those it is safeguarding for others (avoid double counting from other rows above)	£ direct financial loss (e.g. breached bank accounts). £ cost to rework valuable IPR lost. £ loss of any advantage in trading (e.g. commoditisation from imitations arriving or rareness of offer being eroded). £ direct loss of contracts affected.	
Customer, partner, supplier civil suits as a result of contract failure and breach	Consider the contract failure and breach cost.	£ direct cost of loss/consequential loss. £ cost of legal services.	
Regulator and legislator fines	GDPR being the most obvious with up to €20m or if higher 4% of global turnover at risk	£ fine. £ cost of appeals/legal work.	
Reputational consequences leading to financial losses	The impact on your brand and ability to do what you did before	Contract losses not considered above. Share price losses. £ PR recovery costs. £ increase in marketing spend. £ increase in sales costs.	
Remediation costs following incidents	The direct cost and opportunity cost from addressing incidents that arise	£ cost from number of incidents x cost of incident resolution. £ loss of staff time/income in not addressing day job.	
Insurance costs and other related risk premium increases	Cost of insurance is growing due to cyber crime and privacy and may grow further faster if you make a claim	% increase in existing premiums and £ cost. £ of new insurances required e.g. cyber insurance without evidence of an ISMS certification.	
Summary impact from threats	**£** **Notes**		

Opportunities	Considerations for your business case	Value / measure example	Your estimate
Growth within existing customers that believe you are more trustworthy	Avoid double counting from the threat of loss above (assuming straight retention) but consider where you might achieve incremental value	% growth from existing business £ value of growth	
Growth of new customers likely to believe you can be trusted around information security and privacy	The new growth that might come from standing out in your sector for being trustworthy, or by at least keeping up with others who are already ahead	% growth from new business £ value of growth	
Running a better business (for the scope of the ISMS) at lower total cost and risk	An effective ISMS helps identify operational opportunities and threats, areas for improvement and saves resource time	% £ savings for process reengineering / rework in house. % £ savings for management time in admin and decision making.	
Running a better business and having a good reputation for security means attracting better candidates who are more effective (and secure by design themselves)	As the new generation of workers are aware of privacy and cyber threats they want to work in more trusted firms and develop their skills with security by design	% workforce that is secure by its own design and values / beliefs. Savings from reduced cost of training. Savings from reduced cost and volume of incidents.	
More intimate engagement with the supply chain as a responsible customer leads to innovation and reduced cost	Working more closely with suppliers opens up potential for new products, new processes, new markets	£ growth potential from innovation (e.g. new products) with the supply chain. £ savings from lower total of ownership by cutting waste with the supply chain.	
Reduced cost of sales by demonstrating you can be trusted	Avoiding lengthy tender and assurance qualifications exercises around security and privacy credentials (avoid double counting from the threat and focus on the net saving from now)	£ savings from administration around demonstrating security competences to customers and prospects	
Reallocation of resources that are not well utilised from the non-value adding administrative aspects of security work	Time spent managing old fashioned processes, emails, documents, sheets, producing reports, updating management and sitting in meetings	£ benefit from reassigning or enabling specialist security and support staff to focus on new value add areas and work on security improvement not just admin	
Savings and cost avoidance from insurances and related risk premium increases	Insurance companies are getting smarter and whilst premiums are rising generally, they will rise less quickly for organisations that meet better risk scoring profiles e.g. by demonstrating ISMS related certifications	£ direct saving from insurance premiums £ cost avoidance from likely increases	
Summary impact from opportunities	**£** **Notes**		

What is the impact:

- Worst case from the threats?
- Best case from the opportunities?
- Is doing nothing still an option?

'If you believe' (and are in a decision making/budget holding position), no further proof might be necessary to get started with your investment now. 'If you don't believe' (or those who fund the ISMS don't), then consider what proof and presentation is possible/necessary to justify the need and investment for your ISMS.

If you have to produce a more formal case for investment, being clear on the powerful stakeholders and their expectations from an ISMS will be important too.

Let's consider them now.

3.2 Stakeholder expectations for the ISMS given their relative power and interest

Another major factor affecting the investment in the ISMS is to what extent it meets the needs and expectations of stakeholders, given their power to tell you what to do, and their interest in evidence of it being done.

The table on page 32 highlights examples of stakeholders. The common thread is about growing trust through exhibiting confidence and control, where that increases the more visible, insightful and well evidenced the ISMS becomes.

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 able to adapt and grow as this information security and privacy-oriented world changes (because it is changing fast!)

Stakeholder	Interest in the ISMS	Ability to evidence now? Yes / No / NA
Leadership	1. Protection of assets and ability to drive growth in organisation value with confidence in the ISMS 2. Ensuring that information security practice enables business success not prevents it 3. Able to visibly demonstrate the ISMS and build trust with powerful stakeholders 4. Certainty the ISMS is under control and working well at all times 5. The ISMS helps mitigate personal accountability risk as new legislation comes into force 6. The cost of ISMS investments and management of the solution is relative to opportunities and threats 7. Confidence that the ISMS is able to continue working well if people running it change or move on	
Shareholders	8. Confidence that the ISMS is working as expected 9. Protection and growth of shareholder value	
Regulators & Legislators	10. Confidence the ISMS enables privacy and protection of data subject information (e.g. GDPR) 11. Ability to see the actions taken and work done prior to and afterwards - in the event of a breach or reason to investigate (which will influence their recommendations and outcomes)	
Customers	12. Ensuring the organisation delivers on its promises and protects information being shared or processed 13. Evidence that the ISMS is working in the organisation 14. Assurance of the whole supply chain performing especially important suppliers accessing their assets	
External Auditors	15. Ensuring the organisation is running its ISMS according to any agreed standards (e.g. to meet customers' expectations) such as ISO 27001 16. Confidence in the operation going beyond 'tick box' and living the spirit of information security daily	
Employees	17. Protection of their own personal data 18. Reputation of the organisation to continue trading and employ them 19 Ease of demonstrating their personal ISMS awareness & compliance to aid organisation goals	
Suppliers & Partners	20. Confidence that the relationship is not leaving them exposed to risk given supply chain liability is increasing 21. Ability to learn from smart responsible customers & partners about how to protect their part of the supply chain	
ISMS management and administration resources	22. Ease of operation and ability to demonstrate to other stakeholders they are in control of the ISMS 23. Able to focus on 'what' they are doing for improving security and privacy rather than 'how' to build and develop an ISMS itself	
Trade associations / powerful lobby groups	24. Starting to set standards and expectations for organisations in their scope and see evidence of security and privacy best practices from members	

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.

Consider the maturity map on page 33 for the more obvious anticipated outputs and outcomes from the ISMS investment (or lack of it).

Maturity >	GDPR non compliant	GDPR non compliant	GDPR compliant – in your opinion	GDPR compliant with recognised standards	GDPR compliant with independent assurance
Privacy & Regulation focused	No systems, policies, people or technology to support GDPR	No systems, policies, people or technology to support GDPR	Systems, policies, people or technology to support GDPR including own info sec practices eg: • DPO • Clarity of information held • Risk assessment and mgt • Rights of individuals • Information security controls • Staff training and awareness • Supply chain mgt • Incident mgt and BCP • Requests and Assessments	ICO 7 checklists for compliance to GDPR ISO 27001:2013 approaches to replace DIY (goes beyond protecting personal data to a culture of wider infosec)	ICO 7 checklists for compliance to GDPR Full adoption of ISO 27001:2013 (goes beyond protecting personal data to a culture of wider infosec)
Infosec & Certifications focus	None	Cyber Essentials/ Cyber Essentials Plus (CE)	CE + own information security framework (not recognised externally)	CE + ISO 27001:2013 core (excluding parts eg. some mgt requirements, reviews, internal & external audits)	+ Independently certified ISO 27001:2013
Anticipated outcome	Organisation unlikely to survive because of losing its customers or having cyber crime impacts	Increased threat of fines up to 4% global turnover or €20m. Loss of customers likely although less risk from cyber crime	Some stakeholder confidence in compliance, lower loss of business risk, possible cyber crime risk on other information assets (non personal data). Unlikely to 'easily' demonstrate enough confidence to smart or powerful customers	Retaining customers and increasing stakeholder confidence with lower risk of business loss, fines or cybercrime impact. May not win new business from really smart customers without evidence of assurance	Winning new business, retaining customers by stakeholders confident in the organisation with independent audits. Much lower risk and threat from cybercrime or GDPR fines.

STARTING FROM AND GOING TO? THE SIMPLE MATURITY MAP FOR GDPR & INFO SECURITY.

NOTE: THERE ARE RECOGNISED ALTERNATIVES TO ISO 27001 AS WELL BUT NO EU CERTIFICATION STANDARD FOR GDPR YET.

In summary, if the organisation has few powerful stakeholders and a leadership lacking appetite for investment, the ISMS may seek to just cover the fundamentals of privacy to meet regulatory requirements. Basic investments in preventing cybercrime threats such as following Cyber Essentials are useful too.

Depending on those stakeholder expectations and the value at risk, greater returns outweigh the increased investments from putting in place more holistic approaches. This includes following recognised standards such as ISO 27001 or NIST Cyber Security.

The outcomes you want from your ISMS along with the powerful stakeholder expectations will determine the inputs and outputs you need to invest in and the scope of your solution overall.

3.3 Scoping the ISMS to satisfy stakeholder interests

Depending on what the ISMS is aiming to achieve, the scope of the ISMS will vary.

At a minimum the organisation needs to follow applicable legislation and regulation, with examples of increasing demands for regulation-based jobs seen in NYDFS 23500 from the New York Department of Financial Services for cyber security, and Network Information Services (NIS) Directive to protect essential services.

GDPR is also one of the most comprehensive and popular examples of regulation to comply with right now. Doing that well helps go towards the achievement of many other security standards too.

3.3.1 GDPR focused work

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

Work to get done for GDPR*	Ability to evidence now?
Information you hold: • Personal data inventory and understanding of information flows internally and externally through the supply chain • Records processing tracker to demonstrate the privacy and security controls in place	
Risks: Confidentiality, Integrity, Availability (CIA) • Identification & evaluation of risks based on CIA • Ongoing management of risks. Includes demonstration of work being done to them including putting policies and controls in place as well as regular reviews of risks to tolerate, terminate or otherwise address	
Policies and Controls Management: • Individuals rights and privacy policies & controls based on the risks • Information security policies & controls based on the risks • Aligning of policies and controls to recognised standards, certifications and regulations frameworks (where required to meet powerful stakeholder expectations) • Regular reviews of policies & controls, and demonstrating those have taken place • Evidencing the consideration of recommended policies & controls to follow recognised frameworks and checklists such as those issued by the ICO, ISO and others	
Assessments and Requests to ensure privacy & security by design: • Legitimate Interest Assessments • Data Protection Impact Assessments • Subject Access Requests • Rights to object, restrict processing and be forgotten	
Incidents and BCP: • Security Incident Management (including events and weaknesses) • Business Continuity Planning and implementation management	
Staff engagement: • Communications & awareness around privacy and information security – planned and as needs arise • Dynamic & continuous compliance as the organisation changes its policies, controls and practices	
Supply Chain: • Communications & awareness around privacy and information security – planned and as needs arise • Dynamic & continuous compliance as the organisation changes its policies, controls and practices • Contracts, contacts and relationship management • Beyond suppliers into go-to-market partners and others with access to personal data	
Whole System Coordination and Assurance: • Reporting and monitoring of the ISMS performance • Audits and regular reviews with recommendations & resolutions • Evidence based working and integrity of the whole system • Visibility of progress and status at all times	

* There are a large number of activities to be considered for GDPR compliance both in terms of the actual regulation and in terms of meeting compliance with the UK Supervisory Authority (ICO). This aims to simply summarise the main aspects into a consolidated set of 'jobs'. The ICO has 7 checklists with 120 activities listed and the table provides a distilled list of the main elements.

3.3.2 Doing other work for broader security confidence and assurance with higher RoI

Forward thinking organisations are looking beyond just protecting personal data. They are seeing the value of following recognised frameworks such as ISO 27001:2013, or NIST Cyber Security.

A benefit of this approach is being able to more easily demonstrate to stakeholders you can be trusted, and smarter buyers will understand the work you are doing too.

ISO 27001:2013 is even better because you can (if desired) also achieve an independent highly respected certification that helps demonstrate your commitment for stakeholders.

Reflect back on the analysis from the threats and opportunities work earlier. It will almost certainly deliver a higher return on investment (RoI) by extending the scope of information and adopting a recognised framework despite there being a bit more work to do as well.

ISO 27001:2013 has additional work beyond that required for GDPR however there are also lots of synergy areas too. As such, depending on stakeholder expectations (now and in the future) it can make sense to future proof a GDPR investment with an intent towards achieving ISO 27001:2013 as well.

3.3.3 Work to get done for ISO 27001

We always recommend organisations purchase the ISO 27001:2013 standard so they are able to determine what is expected.*

The work to get done from that standard includes describing and demonstrating your approach to the following:

- Evidencing the ISO 27001:2013 management system requirements
- Evidencing controls applied or not applicable from the Annex A control objectives (where there is lots of synergy with regulations like GDPR)

It might seem overwhelming at first glance, and there is a lot to cover if you start from a blank canvas. But once understood it is logical and 'common sense' especially if following a business led approach to ISO 27001:2013 with commitment from leadership. There are many ways to fast track success such as with ISMS.online.

Like most standards, you need to describe what you do to meet it then demonstrate it is happening in practice by showing your workings when required e.g. during audits and reviews with stakeholders.

Covering the management requirements well means all the investment in the relevant Annex A controls will then go towards securely doing business the way you want it to be done, and powerful stakeholders can take confidence from it too. It requires a business led approach to embed into your cultural norms, so please do not let the information security tail wag the dog! Following inappropriate information security advice could mean a much higher risk and cost. It might mean many security-oriented activities are needed before doing the actual task you wanted to do. That will either mean those things don't get done, leaving the business insecure, or the staff do them, and the business has massively slowed down its productivity and effectiveness!

You might also lose key staff too if they don't want to follow practices that are not integrated well with your cultural values and behaviours. (Of course, you may need to change some practices if you are not already demonstrating good behaviours. However, that doesn't mean you need to institute Top Secret Military grade practices for good cyber hygiene in your sector.)

* The ISO 27001:2013 standard can be purchased at: **iso.org/standard/54534.html**
We also suggest you get the ISO 27002 code of practice at: **iso.org/standard/54533.html**

ISO Ref	ISO 27001: 2013 Management system requirements	Activity (work to get done)	Ability to describe & demonstrate now? Yes / No / NA
4.1	Understanding the organisation and its context	The organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome/s of its information security management system	
4.2	Understanding the needs and expectations of interested parties	The organisation shall determine interested parties (stakeholders) that are relevant to the information security management system and the requirements of these interested parties relevant to information security.	
4.3	Determining the scope of the information security management system	The organisation shall determine the boundaries and applicability of the information system to establish its scope. Take into account the external and internal issues (4.1) and requirements (4.2) and interfaces and dependencies between activities performed by the organisation, and those performed by other organisations.	
4.4	Information security management system	The organisation shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of ISO 27001 2013.	
5.1	Leadership	Top management shall demonstrate leadership and commitment with respect to the information security management system.	
5.2	Leadership	Top management shall establish an information security policy that meets the requirements.	
5.3	Leadership	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.	
6.1	Actions to address risks and opportunities	A documented information security risk assessment process, and the treatment thereafter in accordance with that process	
6.1.3	Statement of Applicability	Produce a Statement of Applicability that contains the necessary controls and justifications for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A.	
6.2	Information security objectives	Establish applicable (and if practicable, measurable) information security objectives, taking into account the information security requirements, results from risk assessment and treatment. Determine what will be done, what resources are required, who will be responsible, when they will be completed and how results will be evaluated.	

ISO Ref	ISO 27001: 2013 Management system requirements	Activity (work to get done)	Ability to describe & demonstrate now? Yes / No / NA
7	Resources, competence, awareness and communication	The organisation shall determine and provide resource for the establishment, implementation, maintenance and continual improvement of the information security management system. The resources affecting its performance shall be competent and aware, enabled by relevant internal and external communications.	
7.5	Documented information	The information security management system shall include documented information required by the ISO 27001 and other information determined by the organisation as being necessary for the effectiveness of the system. Creation and updating will include ID and description, format and media along with review and approval, and history of changes. It must be available and suitable for use when and where needed and adequately protected from loss of confidentiality, improper use or loss of integrity.	
8	Operation	Plan, implement and control the processes needed to meet information security requirements and achieve the information security objectives including planned risk assessments and treatments.	
9.1	Performance evaluation	Evaluation of the information security performance and effectiveness of the system. Includes what should be monitored, the measurement, analysis and evaluation, when and who does it, and who analyses and evaluates the results.	
9.2	Performance evaluation	Internal audits to be conducted at planned intervals to provide information on whether the system conforms to the requirements and is effectively implemented and maintained. Demonstrate a plan for the audit programme, with the criteria and scope, selection of auditors, reporting to relevant management and that evidence of the programme and results are retained.	
9.3	Performance evaluation	Top management review of the information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness, using an agenda that considers the requirements of 9.3.	
10.1	Improvement	Demonstrate how nonconformities and corrective actions will be addressed.	
10.2	Improvement	Demonstrate how the organisation shall continually improve the suitability, adequacy and effectiveness of the information security management system.	

You need to be living and breathing points 4.1 – 10.2 in the last table to meet your stakeholder expectations.

In addition to the management requirements there are 114 Annex A control objectives to consider. It's a large number but they are straight forward and common sense, many of which complement the GDPR oriented jobs described earlier too.

At a headline level the Annex A control objectives are broken down as follows:

- A.5. Information Security Policies
- A.6. Organisation of Information Security
- A.7. Human Resource Security
- A.8. Asset Management
- A.9. Access Control
- A.10. Cryptography
- A.11. Physical and Environmental Security
- A.12. Operations Security
- A.13. Communications Security
- A.14. System Acquisition, Development and Maintenance
- A.15. Supplier (and other important) Relationships
- A.16. Information Security Incident Management
- A.17. Information Security Aspects of Business Continuity Management
- A.18. Compliance

You also need to be showing your evidence behind the 114 policies, controls, managing reviews, assessing risks, reviewing and updating policies.

Whilst the work to get done is relatively straight forward, and based around your own risk appetite, there is a lot to do.

Depending on what solution you put in place for the ISMS, its design, implementation, ongoing coordination and management can be unnecessarily costly and might increase risk over time too.

Implementing HR security through the lifecycle, including managing staff compliance to policies, supply chain management practices, security incidents, audits and improvements tracking are just some of the more detailed jobs to get done within this area, all of which dovetail nicely to GDPR too.

Reporting and updating the Statement of Applicability and undertaking the Internal Auditing can be time consuming too.

As such, the solution combination of people and technology for your ISMS is critical, so let's consider that next.

04

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

An ISMS is for life, not just for Christmas, so adopt a sustainable approach.

We have considered the threats & opportunities, where benefits might arise, and the stakeholder's expectations from the ISMS.

That has led to the ISMS deliverables and what work needs to get done as part of the solution.

As long as the organisation is serious about security and goes beyond the tick-box mentality It is probably clear by now that doing nothing is not an option. The RoI is high whichever implementation path is taken.

It is now time to consider the best way to achieve the goals and how to put in place the ISMS itself.

As part of business case cost building it's generally a build versus buy options analysis. Like the benefits / return analysis earlier this investment consideration can be done at whatever level is required for the organisation to feel confident about its decision.

In the next section we look at factors to consider in build versus buy decision making.

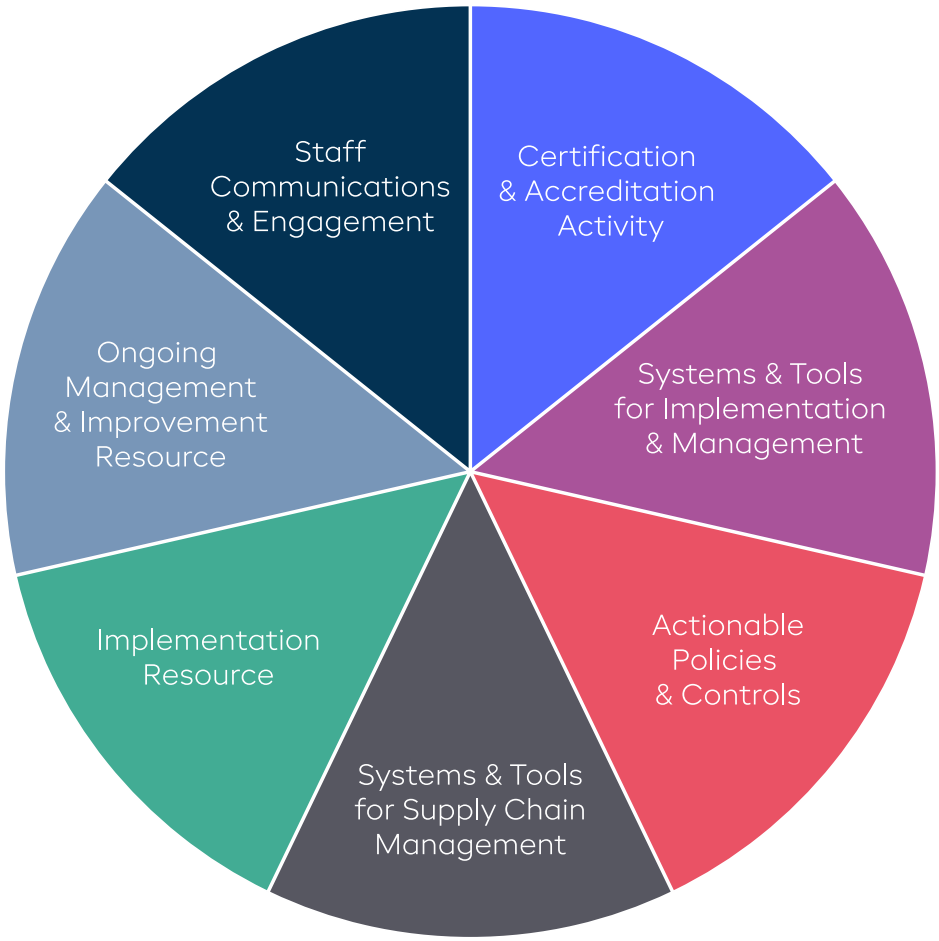
4.1 Understanding the components of an ISMS solution

As touched on earlier, the main components of an ISMS are summarised in the image. The solution is comprised of two main investments to bring it alive:

- People
- Technology

The real size of these pie slices, in terms of time and cost, is all dependent on the objectives, the starting point, the scope of jobs to include in the ISMS, and the organisation's preferred way of working.

Investing well in one slice will help reduce or avoid much larger investments of people or technology in the other slices especially when looking at a whole life cost basis.



Whilst 'content' (your policies and controls documentation) is very important, it's only one component of an ISMS and there are many pitfalls to avoid.

Examples include:

- Purchasing low-cost generic policy documentation may give you a bunch of cheap policies but they will not be 'actionable'. They may even encourage unnecessary work for your organisation.
- Consultants who do the implementation their way without understanding your business practices, or not sharing 'the secret sauce' so you have to use them forever, nor aligning it to recognised standards
- Failure to consider the whole life consequences beyond implementation e.g. dropping spreadsheet documents into a Google folder or Sharepoint style technology system but not considering the ongoing management, coordination, reporting and control requirements for everyone involved.

These approaches will cost much more in the long run, or have big opportunity costs, so consider a total cost of ownership, not just the initial implementation.

4.2 The people involved in the ISMS

Getting the balance of people and technology right is key to meeting all stakeholder's expectations. Too many people or too much time involved, and it will cost too much or have opportunity costs of those resources not delivering value elsewhere.

Not enough people and the ISMS will fail to deliver on its promises, leaving the organisation exposed to the threats, and miss the opportunities identified earlier.

Capacity, Capability and Confidence are the 3 Cs we talk about with customers to ensure that their resources are able to achieve the goals. Typical skills and experiences required for ISMS success include those shown below, where the time required is dependent on the starting point, ISMS goals and the technology solution adopted alongside the people.

- Leadership
- Information security
- Commercial (buy and sell side)
- HR
- Legal
- IT
- Change management

As would be expected there is a higher initial investment in the implementation before settling into a pattern of behaviour over time.

Outsourcing some of that work to specialist consultants can make sense and there is a growing market for 'virtual' and 'on demand' expert support (CISO, DPO* etc), usually enabled by good technology as part of the solution too. Internal leadership should still be involved, and the business must have strong representation in its area of scope to reinforce the culture, values and desired ways of working.

If those people involved in the ISMS are ill equipped or lacking Capacity, Capability or Confidence they can be supported with sustainable and affordable technology, not just more people. Technology solutions such as ISMS.online also offer virtual learning, and pre-configured documentation that is easy to Adopt, Adapt and Add to as it complements the technology platform features, helping drive down total cost and speed time to ISMS success.

* CISO – Chief Information Security Officer
DPO – Data Protection Officer

4.3 The characteristics of a good technology solution for your ISMS

A good ISMS technology solution should be right at the heart of the ISMS.

When combined with the people involved, the whole ISMS is much more easily trusted by those stakeholders.

Technology can not only help to address Confidence, Capacity and Capability issues for the people involved, it will speed time to success, improve visibility, ease coordination, reduce risk and lower the total cost of ownership.

It also helps any external experts you bring in focus on the more specific and challenging parts of your solution.

At a time when it has never been easier or cheaper to throw up a wiki page, build a website, market a service or cobble some code together to solve part of the problem, it is also important to carefully consider what good looks like from a technology solution.

The best ISMS technology solution will meet the 10 characteristics as described over the page.

This list, coupled with the more specific work to get done (as outlined earlier) then becomes your checklist from which to determine whether you should consider building or buying. It is also the specification from which to compare technology solutions on the market.

	Characteristic	Rationale	Existing Solution fit to characteristic? Y/N
1	**Secure** – meeting high independently certified and tested security standards in the application, the organisation that built it, and through the supply chain for hosting and delivery of support	The risks, policies, controls and information held in the ISMS are very important to organisation success! Avoid risks, vulnerabilities and valuable assets being exploited from a poorly built or badly maintained system.	
2	**Always on** – available to authorised parties when and where they want it (with back up and support when needed)	Availability at all times from any (secure) location to demonstrate trust e.g. in front of customers as well as manage the ISMS in real time when needed e.g. following an incident.	
3	**Collaborative** – made for sharing internally & externally to authorised parties	We rarely work alone internally, and increasingly want to collaborate externally too. Without collaborative features embedded inside the ISMS, costs of coordination and sharing can be high, also leaving gaps or duplication across other systems.	
4	**Transparent** – visible, auditable, approval and evidence based to show integrity in the work	Trust is default low and stakeholders want evidence of work done, including the changes over time. You need to 'show your working' as the ISMS evolves in line with business changes.	
5	**All in one place** – configured for all the ISMS work* that needs to get done for the regulations and standards you want to be measured against	People are busy, they don't have time to use and learn multiple systems. Costs of search, knowledge mgt, coordination and contracting all increase with multiple systems. Organisations may not be able to afford or want integration of systems either due to cost/risk/time/complexity	
6	**Joined up** – making engagement and navigation from job to job easy	The person doing some of the input work may not be the same person benefiting from it afterwards. Easier navigation and linking of work reduces cost and offers confidence to stakeholders the ISMS fits together.	
7	**Structured for success** – Encouraging discipline and progress, rewarding small wins, whilst being flexible, extensible & scalable for a fast-changing world	With lots of work 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.	
8	**Insightful & actionable** – with dynamic reports & reminders automatically doing the heavy lifting to avoid admin or rework costs	Stakeholders want visibility and confidence the ISMS is under control. Technology can drive down costs of reminding and reporting, significantly freeing up the people to make better, more timely decisions.	
9	**Easy to use** – and simple to manage regardless of who is involved and how often	Not everyone is a full-time expert and people move on. Infrequent use of an ISMS for some stakeholders means higher costs of use and more likely noncompliance with processes.	
10	**Affordable** – to design, implement, operate and improve	Whilst the returns (addressing the threats and opportunities) are high for a well-run ISMS, the cost of people and technology involved needs to be relative to the value at risk.	

* We describe examples of that work to get done in more depth earlier in the document. They will be determined from your goals.

4.4 Whether to build or buy the technology part of the ISMS

Broadly speaking there are 5 ‘build or buy’ options for the solution and these are:

1. Build your own no-tech paper-based solution

2. Build your own low-tech solution - Email, sheets, docs, shared folders (personal & basic sharing tools)

3. Build (or commission) your own hi-tech specialist software technology solution

4. Buy off the shelf professional standalone applications to do specific ISMS jobs

5. Buy off the shelf professional all in one place ISMS

Its pretty obvious from what ISMS.online offers that we would recommend option 5 - but the other paths all have Pros and Cons which we’ve summarised on the next page.

		Pros	Cons
1	Build your own no-tech paper-based solution	• Avoids most cyber and digital oriented risks	• Does not meet 10 characteristics so may fail on powerful stakeholder expectations • Unlikely to be something anyone seriously considers even within the most sensitive of workplaces • Will likely cost large amounts to maintain and demonstrate compliance against
2	Build your own low-tech solution - Email, sheets, docs, shared folders (personal & basic sharing tools)	• Perceived as free or low cost	• Will be unable to easily meet the scope of all jobs to get done • Does not meet 10 characteristics so may fail on powerful stakeholder expectations • Time required to understand, design, architect, implement and maintain the ISMS structure for all users of it • Higher total cost over life than off the shelf solutions when considering all jobs to get done • Reliance on the person/s who built it to keep it organised and updated as standards change • Unlikely to be a core competence of the organisation to build an ISMS
3	Build (or commission) your own hi-tech specialist software technology solution	• Built to exactly what you want to achieve and the way you want to work • Great if you have very sensitive information management constraints and working practices that other off the shelf solutions are unable to address	• Likely to cost significantly more and take much longer than solutions already in the market in order to meet 10 characteristics • May distract from core competences and cause significant opportunity costs in other parts of the organisation if using limited resources • May mean inability to meet compelling events or deadlines for achieving actual ISMS business goals • Cost of maintaining and improving will be much higher than off the shelf solutions as new standards and regulations emerge (developing for one customer not many)
4	Buy off the shelf professional standalone applications to do specific ISMS jobs	• Use alongside personal and basic sharing tools e.g. documents and spreadsheets • Pick and mix best of breed technologies with cheap / perceived free solutions	• Unlikely to meet 10 characteristics so may fail on powerful stakeholder expectations • Cost of security, coordination, search, integration, contracting and maintaining versions are almost certainly outweighed by an all in one place service • Enhancements in one application do not mean overall ISMS improvement and could make things harder if a vendor releases new features that exist in the other applications
5	Buy off the shelf all in one place ISMS	• More likely to meet 10 characteristics and satisfy powerful stakeholders • Easy to get going quickly with lower costs of contracting, start up and implementation • Use alongside personal and basic sharing tools e.g. documents and spreadsheets • Enhancements and new releases to parts of the ISMS also improve the whole system performance	• All in one packaged solution may not meet the needs of some experts who have a particular way of working (unless custom/bespoke development is undertaken)

4.5 The core competences of the organisation, costs and opportunity costs

However, there is no need to develop the technology solution, unless it is considered a core competence of the firm and resources are on the bench waiting to be utilised.

Some hi-tech technology ISMS solutions cost millions of pounds to build and years to get fit for purpose.

Even lower tech solutions developed with SharePoint or Google folders and files could take weeks or months to bring alive:

- to understand what is required
- to design it
- to implement it
- to manage it
- to keep it updated

All that time may be invested whilst:

- not directly meeting stakeholder expectations
- not achieving all 10 characteristics detailed earlier
- not actually contributing to the business goals behind the ISMS

If you run your sales, accounting and other key business systems using excel sheets and word docs, relying on emails and folders for sharing, then you'll probably want to do the same here.

If you are however serious about information security and privacy, you'll want to show that too with a professional platform in the same way that Salesforce.com. Xero etc deliver for their target audience. Sheets, docs, emails have a role in the ISMS like they do in sales and accounting solutions, but they are not the only thing you need for success.

If your organisation looks at Xero, SAP, Pipedrive, Salesforce.com, MailChimp, Microsoft Office etc and still builds its own hi-tech internal solutions for those areas then you may want to also build your own ISMS too.

If you are considering low-tech or hi-tech build of the ISMS yourself, ask yourself what the organisation's business is and whether that is part of your core business. Is the hourly rate of the resource involved likely to be better focused on the day job?

Even if the organisation develops software for a living, is the time better invested in your core products and services where that may achieve a better return?

Given affordable ISMS solutions exist in the market already, off the shelf, to meet the 10 characteristics, there are only a few reasons why you would want to build one yourself:

- Significant complexity or sensitivity in your organisation information or practices
- Technologies already in place that can be suitably 'bent' to reflect stakeholder goals
- Funding constraints (although even these can be overcome with payment on use and affordability models from some ISMS professional solution vendors)
- A desire to enter the ISMS products and services market yourself

In conclusion

Doing nothing is probably not an option any longer for organisations that want to be seen as serious about information security management.

Deciding whether to purchase a new firewall or implement an ISMS with the current IT budget is missing the point of a more holistic approach to protecting and enhancing organisation value.

Forces for change are growing and powerful stakeholder expectations are increasingly driving towards a more professional ISMS. They already expect you to have a firewall, and are now expecting you to strategically do even more to protect their valuable information.

Treating ISMS as an investment for return rather than just a cost is a great way to help unsure, resistant or laggard leaders to understand the benefits. This document has set out to identify the key areas for consideration as you build that business case.

One size doesn't fit all of course so if you need more help, get in touch with our team at ISMS.online. They or one of our partners will be pleased to assist.

Suggested further reading

ISMS.online blog
Infosec news and expert insight

ISMS.online customer testimonials
Read how our customers succeed with ISMS.online

Why GDPR is a good reason to invest in an ISMS now
GDPR is a powerful external driver forcing organisations to improve data protection and privacy activity

Five steps to GDPR success
A simple approach to GDPR that will allow you to easily demonstrate that you are on the path to GDPR success

ISO 27001 Statement of Applicability: The Complete Guide
Your guide to understanding what a SoA is, who it applies to and why it is important

Alliance Brand: Fulfilling the Promise of Partnering
How to build a successful business by partnering and building alliances

Get in touch

See how ISMS.online can help your business

isms.online
enquiries@isms.online
+44 (0)1273 041140

Why ISMS.online

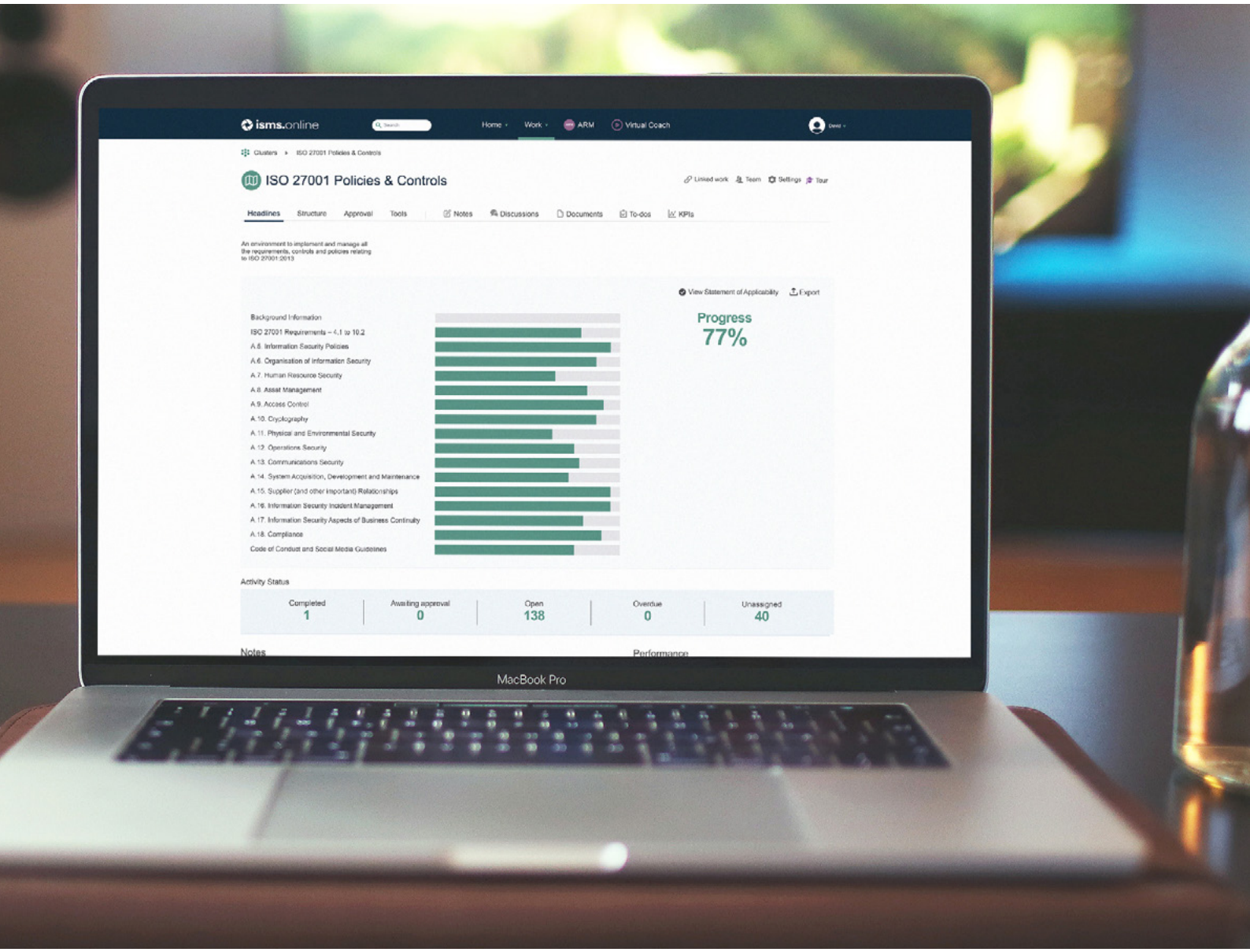
ISMS.online is powerful cloud software that helps deliver an information security and privacy management system your stakeholders can trust at a fraction of the cost, time and risk of alternatives.

ISMS.online is ideal for organisations that are serious about information security, yet don't have the budget and resources for some of the very expensive solutions and hard to use services in the market. It makes the people side of the ISMS equation much easier and more sustainable to solve too whether that is from internal or external sources.

5 reasons why you should consider ISMS.online:

1. It meets all 10 characteristics for the technology part of an ISMS you can trust (see page 48)
2. It enables the work you need to get done for ISMS success around regulations, certifications, standards internally and through your supply chain
3. It comes pre-configured with actionable policies & controls, documentation, frameworks and tools that you can Adopt, Adapt and Add to for a major head start
4. Whether you are new to information security, improving your ISMS or an expert looking to find a better way of working ISMS.online can meet your needs
5. Specialist infosec & privacy partners offer Virtual CISO, DPO and related services inside and alongside ISMS. online if you need them

If you are serious about security then show you mean it with ISMS.online.



isms.online

Still got questions?
Our expert advisers can help:
enquiries@isms.online

Or join the conversation on our socials