

**hicomply**

How to choose the best  
information security  
software for your  
business



## Introduction

There are a wide range of options available for businesses looking to achieve information security compliance like ISO 27001, SOC 2 and GDPR. With so many different solutions to choose from, how do you know which one is right for you?

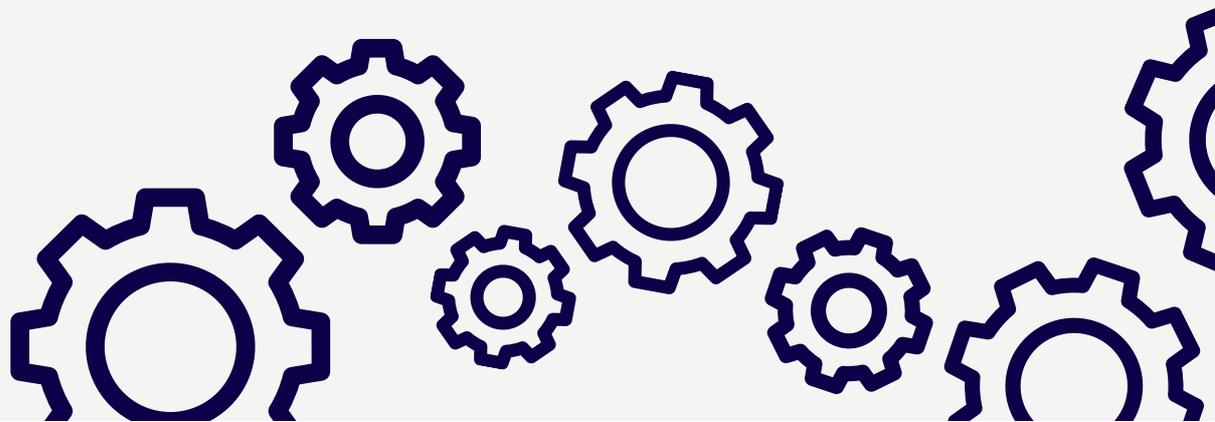
Fear not! Team Hicomply has put together this quick guide. We've included the top 10 questions to ask the GRC and information security software vendors you're weighing up.

### 1. What kind of functionality does the solution offer?

Before going into detail with vendors, it's a good idea to have clearly defined goals. What do you want to accomplish with your digital information security management system (ISMS)? The best platforms offer a flexible suite of configurable tools and features:

- Task management
- Asset management
- Risk management
- Policy and procedure generation
- Document management
- Security controls matrix
- Audit tools
- Reporting and analytics

Also consider if you want the platform to integrate with other systems your company uses. Keep an open mind to learning about each vendor's solution – you may well discover a new feature to add to your wish list.



## 2. Is the software vendor independent in the security certification process?

Ideally, they should be.

However, many security audit firms offer software solutions with the aim of winning audit business. This means the same vendor auditing your business security is also helping manage your security processes. This can cause an issue around independence and arise as a conflict of interest. Accountants, for example, can't audit their own work.

Be wary of vendors that “guarantee” certification to ISO 27001 or SOC 2 in a very short period of time. The audit process should never be guaranteed before it starts - your customers would rightly be very suspicious of certification gained in this way.

In our experience, it's better to work with audit firms that partner with technology vendors but are independent.

## 3. Can the solution be customised?

While every business is unique, most information security managers' needs tend to be consistent across the board. With that in mind, you should easily be able to find solutions that can be configured to your specific preferences and workflows, whether you're managing a single business or a portfolio of businesses in a group.

Many solutions are not easily customised for multiple security frameworks or multiple businesses, so make sure you future-proof your decision.

## 4. How easy is the solution to use?

The answer to this question ought to be “very easy.”

Arrange to see a demonstration of a solution's functionality before your conversation with a vendor gets too far along. One of the primary reasons that



companies end up feeling that their ISMS purchase was an unsuccessful investment is poor adoption rate. If the people who are meant to be using the software don't use it, then you won't realise the return on investment you should.

Every employee, from tech to admin, finance to HR, operations all the way up to C-level managers, should be able to navigate the ISMS on a daily basis.

If the user experience (UX) is too frustrating or confusing, employees may not be thorough in their tasks and errors are likely to occur. You could risk a critical data breach simply because essential information was missing or a procedure not accessible from the system by the staff who needed it.

This doesn't mean that some training on the system won't be necessary, but the solution should still be intuitive with a user-friendly interface. You'll also want to be able to control levels of access and permissions.



**Top tip:** Ask how many support calls the provider usually fields from new clients in the first few months. This will be a pretty good indicator of how user-friendly the solution actually is.

## 5. How long will implementation take?

Depending on how many sites are undergoing transformation and how many applications your chosen package includes, implementation varies from a few months to well over a year. Other factors will also impact the time it takes to get you up and running, including:

- The integrity of your existing data
- The manpower you have available to devote to the project
- How quickly your team is able to learn how to effectively use the system.

Beware of vendors with estimates that are significantly different from the other estimates you've received or that your gut tells you are unrealistic.

## 6. Is the solution a dedicated ISMS software solution or a rebadged document management solution?

A cloud-based ISMS solution, also known as software as a service or SaaS, is usually hosted and managed by the vendor. It is accessed on the internet via a software solution.

There are some vendors who offer what looks like software but often is a file & folder solution using a third party application such as Sharepoint, for example. These solutions look like software but can simply be digital filing cabinets instead - which require a lot of filing!

However, ISMS providers generally have high standards for security, so their storage is most likely as secure as hosting on your own hardware.

## 7. Is the software scalable?

You'll want the software you choose to accommodate unlimited users: those who need to use it now and those who may be added to your workforce in the future. But that's only one way the application should be scalable. Make sure the software you choose can grow with you as your business expands. If you add businesses, assets, or change, can the ISMS software handle the increases and new challenges?

The vetting process is the time to verify a solution's expansion capabilities, so you can be confident that the software will evolve as your company grows.

## 8. Where is the vendor based, where do they host data and where is the technology developed and supported?

Check out each vendor's history and reputation. A reputable provider is going to showcase satisfied customers on their website's testimonials page. If you don't see that information on their site, read reviews on social media. If all the reviews on

review sites are glowingly over-the-top that may be a red flag indicating they aren't from actual customers – many online review sites don't verify review sources.

## 9. What does the vendor offer in terms of training and ongoing support?

If you have been drawn towards the lowest-priced solution in the market, be aware that some ISMS software providers are willing to sell you a solution and leave you to figure out how to use it on your own or limit how much support time you get.

It's best to know up-front what training includes:

- Will they train you on how to set up and show you the ins and outs of the platform features you've selected?
- Is the training included in your monthly fee or an additional setup fee?
- If not, what is the cost for the training?
- Is the training limited to your paid for users?
- Do they have a knowledge base you can search in your own time?

Regarding ongoing support, get the details:

- How are you supposed to contact support—through email, phone or chat communication?
- Are there specific hours that support can be reached?
- Where is support based?
- What is their response time?
- When you call support, will you reach their technicians or is support outsourced?

## 10. What does the cost include?

In today's competitive marketplace, organisations need an edge. An ISMS platform delivers that and more. An ISMS solution should be considered an investment in your company's future.



Things to think about:

- Not all vendors' fee structures are the same – make sure you do your research
- Try to ensure you have a clear understanding of what you will receive for the money you spend
- Usually setup is handled in two different ways: included or extra – make sure to ask which!
- Keep in mind that some systems require technical expertise to set up which can add additional consulting fees. Web-based systems are easier to implement.

It's helpful to know from the beginning how many users you expect to allow access to the new application. Some vendors charge a flat license fee that includes unlimited users.

However, others may charge more as you increase the number of users, which brings up a question of how the vendor defines “user.” Do they consider anyone who simply accesses the system a user, or is it a person who is able to manage tasks and interact with policies and procedures?

## Conclusion: Become a bit of an expert

Research the benefits of information security software on your governance, risk and compliance journey, talk with colleagues in the industry and compare providers. By doing so, you'll be armed with the information you need to make a wise choice when it comes time to selecting the right ISMS software platform.

## Take the fast, simple route to infosec certification

Discover how the Hicomply platform automates 70% of the work for you. Take advantage of free, unlimited onboarding and training for your team, automatic policy and procedure generation, unlimited users and more.

[Buy now](#)

[Book a demo](#)