How is ISO 27001 applicable for Software-as-a-Service companies?

Advisera
Making certification simple.

Table of Contents

Introduction

In today's competitive environment, every customer counts. That's also true if you are providing Software as a Service (SaaS) solutions. But, besides the quality, scalability, and flexibility of the provided services, customers now are carefully looking for providers that can also protect their information better than they can. Considering that, the protection of information integrated with the business, and oriented toward customer satisfaction, is a must.

Implementing an effective and robust Information Security Management System (ISMS) according to ISO 27001 will help you to focus on the important areas of your SaaS solutions and improve efficiency. Processes that are to be established throughout your ISMS will provide a sound foundation to handle relevant risks, leading to increased efficiency and profit. This, in turn, will improve your customer acquisition and retention. Additionally, that makes your management satisfied and your own staff motivated.

In some cases (e.g., public tenders), an ISO 27001:2013 certificate is a must-have. In some other cases, customers will recognize your dedication to excellence in providing high levels of security protection in your SaaS solutions by being ISO 27001:2013 certified. Whatever the situation, even with the cost of the implementation, ISO 27001 brings many benefits to your business.

1. Benefits for a SaaS company

Considering some issues that specifically affect a SaaS business, if you just look at the standard for a moment and think what ISO 27001 can bring to your company, you might be amazed. Here's how your company might gather some benefits:

Fulfillment of Service Levels – The risk management approach of ISO 27001 can help a SaaS provider to decrease the number and impact of most common incidents that can decrease the level of service and/or website uptime, and to monitor service performance, increasing the chances that it will be capable of delivering the expected results at all times.

Continuity of services – Sometimes incidents prove themselves far more critical to a SaaS provider than it can normally handle, causing a complete disruption of activities, and ISO 27001 can provide business continuity capabilities to ensure that the minimum agreed service levels will be maintained, or will be recovered quickly, and that the return to normal operations will be as quick as possible.

Data ownership and control – For customers, just as important as having a SaaS provider to protect their information is the understanding that they, as customers, are still in control of their own information. ISO 27001 can provide a basis for establishing access control functionalities that can be used by the customers themselves to decide who can access their information, and thereby provide better assurance about the data integrity.

Global compliance – SaaS providers have all the world as potential customers, and ISO 27001 can help them identify laws, regulations, and other information-related legal requirements that must be fulfilled for each country they want to have business in, decreasing risks not only to themselves, but to their customers, too.

Proof of excellence on information protection – So, you've set your organization, processes, roles, and responsibilities, and you are achieving excellent results by protecting information. You are also aware that potential customers are looking for best-in-class service, and you have to show them that you are worth their investment. Before they get to know you better, with an ISO 27001 certificate you give them a globally recognized guarantee that they can rely on, until you start delivering evidence of your efficiency once they start using your services.

2. How does ISO 27001 fit to small SaaS companies?

ISO 27001 is a universal standard that can be applied to any organization, regardless of its type, size, or the services it delivers. So, even for small SaaS companies, with their specifics (compared to large organizations), ISO 27001 makes an excellent fit.

The fact that ISO 27001 defines WHAT needs to be done, and not HOW it must be done, to protect information, is its main advantage for small SaaS businesses, because it means that they are not obliged to invest huge quantities of money to start the game.

Broadly speaking, to implement an ISMS based on ISO 27001, smaller SaaS organizations have to:

- Write about 10 to 15 documents to comply with the requirements of the standard and requirements specific to their businesses.
- Train personnel on relevant information security topics (basically teach them to use the developed documentation).
- Spend no money to purchase new software specifically for the ISMS because, in most cases, they already have all the technology they need.

For SaaS organizations up to 10 employees, the ISMS implementation usually takes around three months, with the main person responsible for the implementation spending about 20% of his/her working time on this project.

Enroll in the free webinar ISO 27001: An overview of the ISMS implementation process to see how implementation can be done in an efficient way.

3. How is ISO 27001 applicable for virtual teams?

When we speak about SaaS solutions, most of the talk is about the infrastructure and quality of the delivered service by the SaaS provider. But most new SaaS companies work as virtual teams, where their employees and contractors do not work on the company's premises, but from home offices (sometimes in different countries), accessing the services using different technologies and their own equipment – and, of course, this poses a security challenge, for which ISO 27001 can provide support as well.

In this scenario, ISO 27001 can also be used to identify risks related to access of information being performed from off-site and using devices not owned by the organization, with the implementation of controls such as:

- Acceptable use of assets, to ensure there are clear rules for all employees and contractors for the use of information systems and other information assets.
- Terms and conditions of employment, to ensure roles and responsibilities for information security are formally understood and accepted (strangely enough, the most common security incidents are not related to intentional attacks, but to a lack of awareness of information security responsibilities and the consequences to the person or organization if information security is compromised).
- Security of equipment and assets off-premises, to ensure that proper controls are implemented to handle the risks of working outside the organization's premises (e.g., restrict access to rooms, not leaving equipment unattended, etc.).
- Agreements on information transfer, to ensure there are clear rules to protect the security of information when it is exchanged within or outside of the organization.

In short, with ISO 27001, a SaaS company can protect not only the assets inside its premises, but also define proper rules to ensure the protection of information when being accessed by virtual teams, wherever they are working from.

4. How to set the scope if the server is in the cloud

The scope definition of an Information Security Management System (ISMS) requires clear understanding about what to protect to minimize the risks of information compromise, and servers implemented in cloud environments are an extra challenge in this critical step of the ISMS implementation.

While the flexibility of cloud solutions offers many options for an organization to choose from to fulfill its needs, these can also result in different risk scenarios that can have a great influence over the scope definition itself.

The following are the most common cloud solutions you can find, in order of increasing complexity:

Infrastructure as a Service (IaaS): offers only basic computing infrastructure (e.g., physical and virtual machines, location, network, backup, etc.)

Platform as a Service (PaaS): offers, beyond computing infrastructure, a development environment for application developers (e.g., operating systems, programming language execution environment, databases, etc.)

Software as a Service (SaaS): offers to final users access to application software and databases (e.g., email, file sharing, social networks, ERPs, etc.)

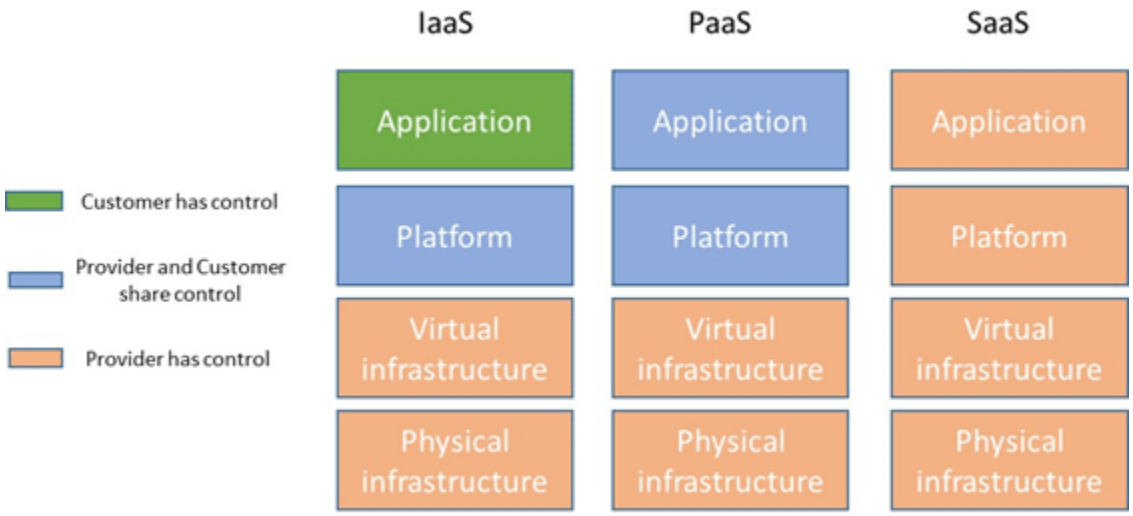

Figure 1 – Asset control by cloud service models

Note that, as complexity increases from IaaS to SaaS, assets under the control of the customer start to go under the control of the provider, and this drives the changes in the ISMS scope, as will be presented next.

Considering these cloud solutions, here is how to take them into account to ensure that an ISMS scope based on ISO 27001 is aligned with business needs and the adopted cloud solution, covering the information to be protected:

Cloud Solution	Comment	Impact on ISMS scope definition
1) The organization deploys its physical servers to host their virtual servers on its own datacenter.	This is the private cloud type concept, more often seen in medium and large organizations, who can afford the infrastructure costs. In this case, the cloud model (IaaS, PaaS, or SaaS) does not have influence over the scope, as all assets belong to the organization.	Datacenter facilities' physical location, hardware, software, and data should be included in the ISMS scope.
2) The organization deploys its physical servers to host their virtual servers on a third-party infrastructure (only space and facilities).	The third party offers colocation service (a widely used outsourcing concept before the age of cloud services) and the organization operates the physical and virtual servers. This can be seen as a transition between private and public cloud types.	Hardware, software, and data should be included in the ISMS scope, while the physical location is out of the scope.
3) The organization deploys its virtual servers in a third-party basic computing infrastructure (public IaaS).	The organization takes advantage of all physical infrastructure and virtual machines provided by the third party.	Software and data should be in the ISMS scope, while physical location and hardware are completely out.
4) The organization uses a third-party platform (public PaaS).	Virtual servers and, to some degree, applications are provided by the third party.	When the organization uses a third-party Platform-as-a-Service, the data and all application software should be included in the ISMS scope, while everything else is out, including all system software.
5) The organization uses third-party Software-as-a-Service (public SaaS).	Virtual servers and all applications are provided by the third party.	When the organization uses third-party Software-as-a-Service, only the data should be in the ISMS scope.

As you can see, the adopted cloud solution can greatly impact an ISMS scope, from having everything under your control to only maintaining the data with you. But, what does this reduction in scope mean in terms of risks? Does this mean that you will have fewer concerns about information security? The short answer is no.

Just because you have another entity responsible for elements you used to control does not mean the risks disappeared. This situation, when you designate another party to handle your risks, is called risk transfer, and can be adopted when the results of the risk assessment demonstrate that a third party can provide a better solution than you handling the assets yourself. For more information, see: 4 mitigation options in risk treatment according to ISO 27001.

But the benefits may be rendered useless if the third party's practices do not offer proper security levels considering the organization's scope. To handle this situation, an organization should consider ISO 27001 controls related to supplier relationships (Annex A, section 15), for example, by establishing security clauses in contracts and service agreements. For more information, see: 6-step process for handling supplier security according to ISO 27001.

For more information about the size of the scope, see Problems with defining the scope in ISO 27001.

5. How does the certification process work?

Once you have decided to go for the ISO 27001 certification and completed all the necessary activities and investments, how will you know if you have everything the certification body is asking for? What exactly will the auditor be looking for?

First, the auditor will perform the stage 1 audit, also called the "document review" – in this audit, the auditor will look for the documented scope, ISMS policy and objectives, description of the risk assessment methodology, risk assessment report, statement of applicability, risk treatment plan, procedures for document control, corrective and preventive actions, and the internal audit.

You will also have to document some of the controls from Annex A (only if you found them applicable in the Statement of Applicability) – inventory of assets (A.7.1.1), acceptable use of assets (A.7.1.3), roles and responsibilities of employees, contractors and third-party users (A.8.1.1), terms and conditions of employment (A.8.1.3), procedures for the operation of information processing facilities (A.10.1.1), access control policy (A.11.1.1), and identification of applicable legislation (A.15.1.1). Also, you will need records of at least one internal audit and management review.

If any of these elements are missing, this means that you are not ready for the stage 2 audit. Of course, you could have many more documents if you find it necessary – the above list is the minimum requirement.

The stage 2 audit is also called the "main audit," and it usually follows a few weeks after the stage 1 audit. In this audit, the focus will not be on the documentation, but on whether your organization is really doing what your documentation and ISO 27001 say you have to do. In other words, the auditor will check whether your ISMS has really materialized in your organization or is only a dead letter. The auditor will check this through observation, interviewing your employees, but mainly by checking your records. The mandatory records include education, training, skills, experience and qualifications (5.2.2), internal audit (6), management review (7.1), corrective (8.2) and preventive (8.3) actions; however, the auditor will be expecting to see many more records as a result of carrying out your procedures.

Please, be careful here – any experienced auditor will notice right away if any part of your ISMS is artificial and is being made for the purpose of the audit only.

OK, you knew all this, but it still happened – the auditor found a major non-conformity and told you that an ISO 27001 certificate will not be issued. Is this the end of the world?

Certainly not. The process goes like this – the auditor will state the findings (including the major non-conformity) in the audit report and give you the deadline by which the non-conformity must be resolved (usually 90 days). Your job is to take appropriate corrective action, but you have to be careful – this action must resolve the cause of the non-conformity; otherwise, the auditor might not accept what you have done. Once you are sure the right action is taken, you have to notify the auditor and send him/her the evidence of what you have done. In the majority of cases, if you have done your job thoroughly, the auditor will accept your corrective action and activate the process of issuing the certificate.

It is important to note that the certificate is valid for three years only, and it can be suspended during that period if the certification body identifies another major non-conformity on the surveillance visits.

Conclusion

With core technologies becoming more accessible each year, and the range of available solutions increasing, cloud solutions providers now have to find alternative ways to offer possibilities for their customers to make their business run in a more cost-effective way – and offering higher levels of information security may prove a great differential. But you should be aware that the benefits for you as a SaaS provider, and to your customers, can be lost (or even result in further damage) if your cloud scenario is not considered in the way you protect information under your responsibility.

By following the requirements and controls of ISO 27001, you can form a solid basis for defining your organization's ISMS scope and the sharing of responsibilities between you and your customers. This will help you plan the controls and clauses you will offer as differentials for your cloud services, allowing you to attract and retain more customers and ensure the sustainability of your business as a SaaS provider, while keeping information and assets under your responsibility properly protected.

Sample documentation templates

Along with the individual document samples referenced in this document, there are more documents available to help you implement ISO 27001:2013 for cloud environments more easily – see this ISO 27001 Documentation Toolkit, which contains all policies and procedures required by the ISO 27001:2013 standard, along with the most commonly adopted documents for an Information Security Management System.

References

27001Academy

About the author

Rhand Leal has 14 years of experience in information security, and for 6 years he has continuously maintained a certified Information Security Management System based on ISO 27001.

Rhand holds an MBA in Business Management from Fundação Getúlio Vargas. Among his certifications are: ISO 27001 Lead Auditor, ISO 9001 Lead Auditor, Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), and others. He is a member of the ISACA Brasília Chapter.

27001 Academy

ISO 27001 and ISO 22301 Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020

EXPLORE **ADVISERA**

9001 Academy
9100 Academy
13485 Academy
14001 Academy
16949 Academy
45001 Academy
20000 Academy
27001 Academy
EUGDPR Academy
Conformio
eTraining
AdviseraBooks

Advisera
Making certification simple.