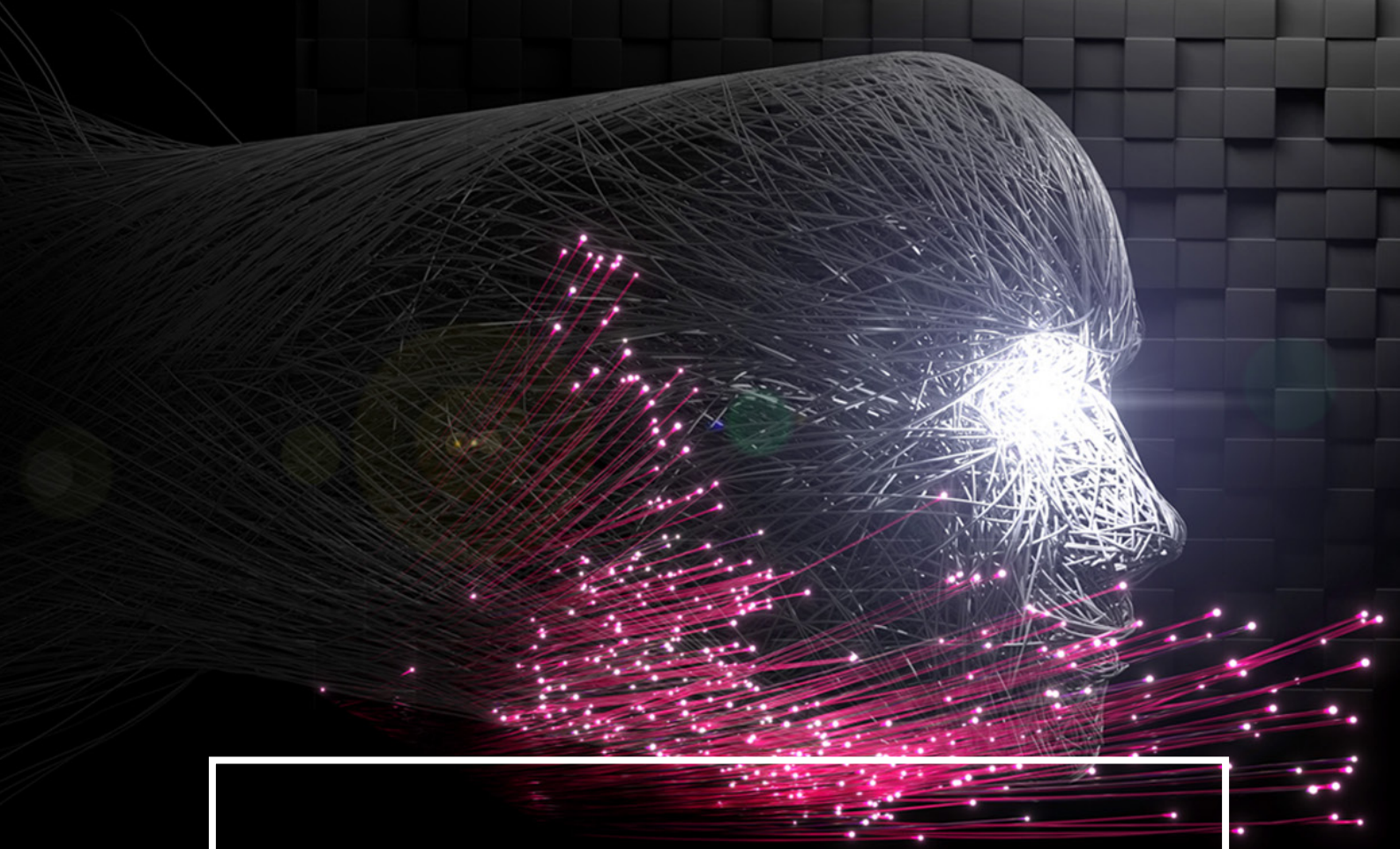


EYRAPPROACH

How to efficiently implement ISO 27001 for cloud-based companies?

Table of Contents

Executive summary

Nowadays, we are seeing more and more companies adopting cloud-based technologies, either as consumers or providers of cloud services.

However, there are still information security risks that need to be addressed when working in the cloud.

As well as a need for secure solutions, there is also a business need for trust and assurance of data protection and business resilience.

Both as consumers and providers, it is important to provide these assurances and an ISO 27001 certification can help achieve that goal.

In this article, we will

- Help companies navigate their way through the implementation of an ISO 27001 compliant ISMS.
- Clarify roles and responsibilities: although the risks may be transferred to the cloud provider in certain cases, an organisation remains accountable for data protection and privacy.
- Identify which clauses of the Annex A controls need to be adapted for cloud-based companies and compare the difficulty to an on-premises model.

Foreword

What is our goal?

With this article, we aim to provide guidance for cloud-based companies contemplating ISO 27001 certification as well as advice based on real case experience.

As you'll discover, if well-conceived from the start, certification can be powerful and reduce operational overhead.

Who are we addressing?

1. Firstly, this paper addresses companies looking to achieve the ISO 27001 certification as well as those simply looking to implement an ISO compliant ISMS.

2. Secondly, we are addressing both cloud consumers and providers. Whether consuming or providing cloud services, it is your organisation's responsibility to guarantee the protection of the data you process. This responsibility also extends to your providers.

   So as a cloud consumer, to achieve certification, it falls on you to ensure your provider is also compliant with all requirements relating to your data.

3. Lastly, SMBs, including start-ups and scale-ups, who are choosing a cloud model do not always have a CISO or a dedicated IT Security Manager.

   Therefore, this paper also addresses both the business and technical teams of cloud-based companies. It provides some high-level insights as well as more technical content designed to help smaller companies, without an extensive security department, navigate the certification process.

Introduction

What are the benefits of an ISO 27001 certification?

Organisations pursuing an ISO 27001 certification are looking to demonstrate the security maturity of their environment, their processes and to create trust and confidence towards the market.

Getting ISO 27001 certified is a fantastic business-enabler and is also a powerful marketing tool, as a seal of quality, generating a competitive advantage.

An indirect benefit of the certification is an increased maturity level. The process requires companies to define and therefore improve internal processes which leads to a more mature, more secure set-up.

What are the challenges?

Although there are many benefits to getting certified, most organisations consider an ISO 27001 compliant ISMS a big commitment in terms of time and resources.

One of the biggest challenges is that the ISO27001:2013 controls (Annex A) do not consider digital transformation. Therefore, on its own, the standard isn't adapted to today's cloud environment.

Requirements:

- Implementing new processes
- Assigning new roles
- Creating information security policies
- Developing process documentation
- Allocating resources while new business requests continue to grow

Therefore, additional implementation guidance such as the ISO 27017 (standard developed for cloud service providers and users), or the ISO 27018 (code of practice for the protection of personally identifiable information (PII) in public clouds) or even the new ISO 27701 (relating to a Privacy Information Management System) are published to take digital transformation and privacy into account.

So how can the ISO 27001 standard be adapted to build an efficient ISMS (Information Security Management System) for cloud-based companies?

Fortunately for cloud-based companies, several clauses, requirements and controls defined in ISO27001 Standard can be smoothly implemented, reducing the feared burden.

DISCOVER HOW

Cloud-based companies

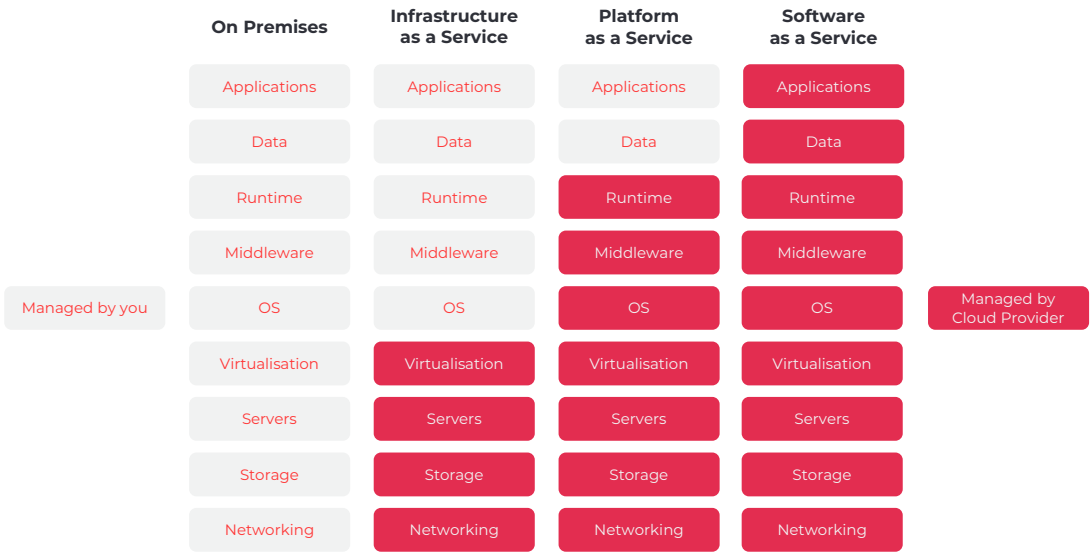
When referring to cloud-based companies throughout this document, we include organisations that are cloud consumers, providers or both unless clearly specified otherwise.

In any case, the company looking to be certified is accountable for the protection of its data and business.

Before deep diving into the ISO 27001 certification requirements, we would first like to cover some more general points that directly impact a company's security.

Responsibilities and accountability between consumer & provider

Organisations need to have a clear understanding of the distribution of security relevant roles and responsibilities with their chosen Cloud Service Provider (CSP).



Depending on the organisation's chosen service model (IaaS, PaaS, Saas) and whether the organisation is itself providing cloud services (mostly SaaS), the share of responsibilities will vary greatly between SaaS offerings and IaaS offerings, with the latter delegating more responsibility to the customer, as seen in the summarised figure above.

It is important to remember that even though the risks may be transferred or shared with the cloud provider, the organisation remains accountable for the protection of their data and business services.

Cloud-based companies

It is vital that businesses perform their due diligence when selecting a CSP, their deployment model whether public, private or hybrid, as well as community and service models (IaaS, PaaS, SaaS), to ensure they are adhering to the company's security requirements.

The general lack of understanding of responsibilities and accountability leads to information security and privacy protection either not being implemented correctly according to your business requirements or not being implemented at all.

Example:
Depending on the cloud model, the provider will assume responsibility for back-ups and business continuity requirements for the services they provide but not for your back-up. Hence the need for organisations to clearly understand their roles and responsibilities.

Security Requirements

For cloud providers (most likely SaaS) in a B2B or B2C context, it is necessary to define the security requirements based on the company's stakeholders' – primarily customers – interests. These requirements may include items such as geographical constraints, data classification and processing, availability, ... It is therefore important to choose a CSP (IaaS or PaaS) which will be able to also meet a maximum amount of these requirements.

As a cloud consumer, trying to impose security requirements on larger CSPs will most likely be an impossible endeavour. Either the organisation accepts the CSP's standard terms and conditions, or it simply couldn't subscribe to the CSP's services.

Smaller CSP players might be somewhat more flexible and are more likely to accept an organisation's specific requirements in terms of security. However, they may not offer the same level of resilience as larger CSPs, which is an important criterion for a business to consider.

Due diligence

As a cloud consumer, the CSP most likely being a critical supplier, the organisation needs to be in control and monitor its performance (A.15.1 and A.15.2):

- Ensuring the services are rendered according to the subscribed services,
- The availability is monitored via external sources,
- The CSP still holds a certification like ISO 27001, SOC2 or other, ...

It is the organisation's responsibility to verify that the CSP is properly respecting their security requirements when looking to be certified.

How to build a smooth and efficient ISMS?

Getting started

No matter the company model; before starting the implementation of an ISMS, it is mandatory for the organisation to complete a thorough risk assessment, taking the scope, internal/external issues and objectives into account.

Risk assessments are perceived as the most complex and incomprehensible part of ISO 27001, but they represent the most important step of a successful implementation as they allow organisations to quickly identify their risks.

According to the ENISA report « Benefits, risks and recommendations for information security »[1], the top cloud security risks are loss of governance, lock-in, isolation failure, compliance risks, management interface compromise, data protection, insecure or incomplete data deletion and malicious insiders.

With today's available tools - whether Open Source, paid application or add-on – the risk assessment exercise can be completed in a short period of time and can easily be replicated.

How to build a smooth and efficient ISMS?

Implementing an efficient ISMS

Whatever model an organisation chooses (cloud, on-premises or hybrid), there are a series of requirements the organisation must meet to get certified.

The ISO 27001 Standard contains, in its Annex A, 14 clauses pertaining to control objectives and security controls (safeguards).

Some clauses are unaffected whether the organisation uses a cloud-based or on premises model and have the same requirements.

In the table below, the implementation difficulty for each clause is identified. If the requirements are not the same for both models, then the implementation is rated as either 'easy', 'Moderate' or 'Difficult' to provide a clear comparison of the effort required for each clause.

Clause	On-Premises	Cloud-Based
A.5. Information Security Policies	Same requirements	
A.6. Organisation of information security	Same requirements	
A.7. Human resource security	Same requirements	
A.8. Asset management	Same requirements	
A.9. Access Control	Same requirements	
A.10. Cryptography	Moderate	Easy
A.11. Physical and environmental security	Moderate to Difficult	Easy
A.12. Operations security	Difficult	Easy
A.13. Communications security	Moderate	Easy
A.14. System acquisition, development and maintenance	Moderate to Difficult	Moderate
A.15. Supplier relationships	Moderate	Easy
A.16. Information security incident management	Same requirements	
A.17. Information security aspects of business continuity management	Moderate	Easy
A.18. Compliance	Same requirements	

Implementation difficulty ratings are subject to organisations' implementation willingness, existing processes, technology used and other factors...

How to build a smooth and efficient ISMS?

Adapting to a cloud-based model

As mentioned previously, for cloud-based companies, several of the clauses can easily be implemented. Indeed, the burden of numerous requirements is placed – either fully or partially – on the Cloud Service Provider (CSP).

Hereafter are examples of clauses that can be either fully or partially managed by the CSP.

Capacity Management (A.12.1.3)

On-premises server management requires well-designed Capacity Management, where the input comes, ideally process-wise, from the business and can be anticipated to ensure enough memory/CPU/disk capacities are planned and will be available for future customer requirements or projects. Sudden and unexpected requests for capacity increases can put operations in deep trouble and slow down business operations.

Whereas in cloud environments, depending on the XaaS subscription, the capacity is managed simply by using a cloud service provider's auto scaling capability, e.g., Amazon EC2 Auto Scaling, where the capacity automatically increases or decreases based on load or other pre-defined metrics or thresholds. The organisation is accountable for the capacity management monitoring.

Hardening (A.14.2.5)

Hardening of on-premises servers is subject to hardening policies, processes, validation by the CISO, continual updates and configuration changes. Whereas in a cloud environment, the CSP proposes hardened Virtual Machines.

With AWS (Amazon Web Services), you create an automated process that builds and deploys hardened AMIs. It is hardened in accordance with the associated CIS Benchmark that has been developed by consensus as being the industry best practice for deploying a secure configuration while reducing cost, time and risk.

Google (GCP – Google Cloud Platform) proposes CIS Hardened Images as well, which are virtual machine images pre-configured according to the security recommendations of the CIS Benchmark.

CIS Hardened Images are also available in Microsoft Azure Marketplace.

How to build a smooth and efficient ISMS?

Monitoring and consequent dashboarding (ISO 27001 9.1 Monitoring, measurement, analysis and evaluation)

Monitoring and dashboarding of on-premises servers requires multiple tools to be implemented. CSPs offer numerous monitoring functionalities, dashboarding capabilities and alerting features.

All of which are needed to demonstrate compliance, manage the infrastructure and monitor the cloud service provider.

Physical and environmental security (A.11)

Companies, most often smaller ones, sometimes rent open spaces or co-working places where employees can meet, communicate, brainstorm and operate.

The physical and environmental clause of the Annex A can easily be implemented since the organisation relies on the security provided by the building owner, at least if in-line with their requirements.

Therefore, a light security assessment is needed to ensure that access to the building and dedicated spaces is in-line with the organisation's expectations (e.g., badge or fingerprint system) and that the network security is configured and managed in a secure way (i.e., default admin credentials changed, WAP2 activated...).

From an environmental perspective, the spaces should be protected against natural disasters (e.g., flooding, power outages, fire, ...).

Documenting the measures in place to ensure the physical security will suffice for this clause. A short information security policy is also needed (i.e., Clean Desk and Clear Screen Policy) to further mitigate physical security risks.

How to build a smooth and efficient ISMS?

Resilience (A.17)

When it comes to resilience, CSPs provide several means to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources.

Organisations seeking certification will simply need to document what is foreseen in terms of business continuity (disaster recovery site(s) involved) and how security is ensured even in adverse situations, under the provision that recovery tests of critical systems have been done and can be proven.

So, the time of IT operators dumping data from physical servers onto magnetic tapes, encrypting and labelling them before sending them to a third party specifically contracted for this operation is practically over, except for some specific cases or circumstances. Furthermore, the burden of restoring tapes and testing them is becoming an obsolete activity.

Nonetheless, there is still a need to demonstrate that back-ups have been made or data synchronized, following the outcome of the BIA (Business Impact Analysis) and its RTO/RPO[1], that restores have been done based on an annual plan and all activities are documented i.e., by using the back-up tool functionalities (logs).

[1] RTO = Recovery Time Objective
RPO = Recovery Point Objective

How to build a smooth and efficient ISMS?

After implementing an ISO certified ISMS

Once the implementation of the ISMS is complete and the organisation receives its ISO 27001 certification, the journey is not over.

Far from being a one-off exercise, a certification needs to be renewed and the internal processes continuously improved to stay certified.

Whether using internal resources or relying on external cyber security experts, it is important for companies to invest in the maintenance and continual improvement of an efficient ISMS and continue to adhere to ISO 27001 requirements.

When to use an external provider?

Often, organisations are not quite familiar with all the terms, concepts and management processes as described in the ISO 27001 Standard. Terms like asset, threat, control objective, risk criteria... need to be explained.

Also, the implementation of a framework like ISO 27001 is a long way from the organisation's daily activity and business. The support of an external company providing services and solutions covering the entire cyber security value chain, from governance and strategy, through resilient technical designs and implementation, helps organisations reduce the ISO 27001 implementation time and manage the certification process.

When the organisation is certified, the support of cyber security professionals is greatly beneficial to ensure the ISMS is still running efficiently, improved and monitored but also to ensure the risks are mitigated and the attack surface is minimised.

EYRApproach offers its services, comprehensive solutions, deep expertise, proven methodologies to support companies looking to implement a smooth but efficient ISO 27001 compliant ISMS while reducing their cyber risks.

Conclusion

Whether on-premises or cloud-based, Implementing an ISMS compliant with the ISO 27001 Standard can be a long journey. Independent of company size and model, the process will take several months.

Usually, after implementation, the ISMS then needs to be in the “Run” phase for at least 3 months before an organisation can claim its ISMS is operational, producing the expected outcome and certifiable.

And although the ISO27001:2013 Standard is not designed specifically for cloud-based companies, it can easily be adapted as demonstrated above. Most controls of the Annex A are even simpler to implement in a cloud environment as the responsibilities are shared with the CSP.

However, it is important to remember that even though the responsibility is shared or transferred to the provider, the accountability always remains with the company.

The Return on Security Investment (ROSI) clearly leans toward cloud solutions because of their flexibility, reliability and security. It removes all worries regarding maintenance, updates, obsolescence of systems and allows IT teams to focus on the essentials to support the core business.

Adopting a cloud-based model, if properly assessed during the risk analysis and due diligence, can be an enabler for an ISO 27001 certification rather than a hindrance.

Final word

Is the ISO 27001 standard the right answer to today's cyber security threats?

Getting an ISO 27001 certification will not prevent cyber-attacks. Businesses will better protect their digital data but alone it is not enough. To complement an ISO 27001 certification, it is important to also ensure the organisation is able to anticipate, prevent, protect, detect/respond and recover. This 360° approach will ensure the right security strategy is in place and meets the security objectives while offering customers reliable and resilient cloud services.

The ISO 27001 focuses on an Information Security Management System. However, as mentioned in the beginning, the standard alone does not consider digital transformation and the cloud environment.

Therefore, in addition to the ISO 27001, the implementation of controls from the ISO27017:2015 Standard (guidelines for information security controls applicable to the provision and use of cloud services) should also be considered to lower the attack surface and move from 'basic' to 'good' cyber hygiene as defined by the CMMC (Cybersecurity Maturity Model Certification) model.

To be complete, it is important to mention other standards that might be relevant for organisations using the cloud and for organisations seeking to protect PII (Personally Identifiable Information) :

- **ISO27017:2015** Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- **ISO27018:2019** Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- **ISO27701:2019** Privacy Information Management System (extension to ISO/IEC 27001 for personal data protection)

Other frameworks to consider:

- CCM – Cloud Control Matrix issued by the Cloud Security alliance (CSA)
- NIST – National Institute of Standards and Technology SP 800-53 (Security and Privacy Controls for Information Systems and Organizations)

Considering the speed of technologies, regulations and cyberthreats, selecting the most appropriate norms/standard for your business might be complex. Getting support from experts will help you benefit from the best approach to cloud security challenges.

Why EYRApproach?

About the author

Marc Degembes is a confirmed ISO 27001 certified Senior Lead Implementer, working since 2014 for Approach. Marc successfully supports various SMBs to become certified by using proven methodologies ensuring a pragmatic and sized approach in-line with the organisation and its business.

"The implementation of an ISMS is greatly simplified for cloud-based companies, but even if the main goal of the organisation is the certification itself, the focus shall remain on the ease to maintain and improve it while controlling the risks and reducing the attack surface."

About EYRApproach

EYRApproach, a joint venture between Eyra Group Switzerland and Approach Belgium, is a pure-play cyber security and privacy firm.

For more than 20 years, we have been building trust in the cyberspace and helping our clients deal with cyber-attacks, incidents and breaches.

We offer 360-degree solutions to improve your cyber resilience: anticipate, prevent, protect, detect, respond and recover.

EYRApproach provides tailored and local services matching your needs: consulting and audit services, training and awareness, security technology implementation and development services, and outsourced Managed Security Services thanks to our own Security Operations Centre (SOC).

We are a scaleup company with a team of a hundred people spread across several sites in Belgium and Switzerland. Our company is ISO 27001 certified and ISO27701 verified.

www.eyra-group.ch

Thank you!

EYRApproach Geneva

Chemin de Place Verte 34
1234 Vessy
Switzerland

EYRApproach Lausanne

Avenue des Baumettes 9
1020 Renens
Switzerland

EYRApproach Zürich

Seestrasse 54
8806 Bach
Switzerland

EYRApproach Neuchâtel

Av. des Champs-Montants 12b
2074 Marin-Epagnier
Switzerland

Approach Louvain-la-Neuve

Axis Parc
Rue Edouard Belin 7
1435 Mont-Saint-Guibert
Belgium

Approach Antwerp

Pamica Building
Rouaansekaai 1
2000 Antwerp
Belgium

www.eyra-group.ch

info@eyra-group.ch

Follow us: EYRA Group 360° IT Services

EYRAPPROACH