

PUBLIC CLOUD SECURITY

Strategic choices for a **secure IT environment**

Content

Introduction	3
Public cloud: a different mentality	4
Fundamental choices	6
Network framing	8
Security at application level	10
Protection against external threats	12
The human factor	14
Continuous guarantee	17
Conclusion	18
You may also be interested in	19



In the 2nd quarter of 2022, the average number of weekly cyber attacks in the Netherlands rose by 40% compared to the same quarter last year.

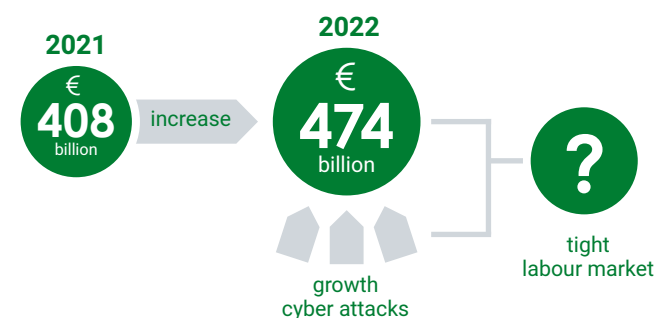
Introduction

Whether you're the CEO, CISO or CTO, the question remains the same: how do you maximise the business benefits of the cloud? Business processes and services are increasingly cloud-based. And with good reason: switching to the public cloud can generate many benefits, such as more flexibility, greater efficiency, improved performance, higher potential for innovation and further development, and less management. Not surprisingly, turnover from cloud activities is growing substantially. [Gartner estimates](#) that global cloud revenues will reach \$474 billion in 2022, compared to \$408 billion in 2021. What's more, Gartner analysts expect cloud revenues to exceed non-cloud turnover in IT markets in the coming years.

Yet at the same time, organisations are faced with significant challenges. Threat levels are rising, for example. [The number of cyber attacks](#) has been growing for years. In the 2nd quarter of 2022, [the average number of weekly cyber attacks in the Netherlands](#) rose by 40% compared to the same quarter last year. In addition, according to the same source, the number of ransomware attacks increased by 59% compared to last year. And the attacks are getting increasingly sophisticated. The days of the lone hacker are over, you now do battle with well-funded cartels.

And the lack of knowledge does not help. [The IT labour market is faced with a significant shortage](#), which logically leads us to conclude that the number of security specialists able to deal with modern cyber threats is not sufficient to provide every organisation with in-house knowledge. The need for a sound security strategy is therefore becoming increasingly clear, a strategy that goes beyond IT alone and that must be continuously adjusted as market conditions change.

And it's within this field of tension that you have to find your way to the cloud. So despite these challenges, how do you properly integrate security into your digital transformation towards the public cloud? This white paper discusses the key focus points and pitfalls for a secure public cloud environment.





Public cloud: a different mentality

When you first enter the public cloud, you enter a new world. The traditional IT environment is inward-facing, shielded from the outside world and designed for internal access. Unlike private environments, public cloud endpoints are designed to be accessed from the outside world.

A public cloud environment is structured differently. Private environments require preliminary work when, for example, the infrastructure needs to be purchased or scaled up, whereas in a public cloud you can switch something on or off with a few lines of code. That flexibility is one of the great advantages of the public cloud. Yet with that flexibility comes more complexity due to the

many functionalities that are available. A mistake in the settings is easily made, which inadvertently opens an environment to the outside world, or activates certain features, resulting in high costs.

In order to use the flexibility of the public cloud safely, the trick is to define frameworks, or guardrails if you will, within which you remain agile. That's a big shift in mindset when you come from a traditional private cloud environment. It's a shift that goes far beyond technology and one that affects all aspects of the organisation, ranging from strategic decision-making and HR to IT management.

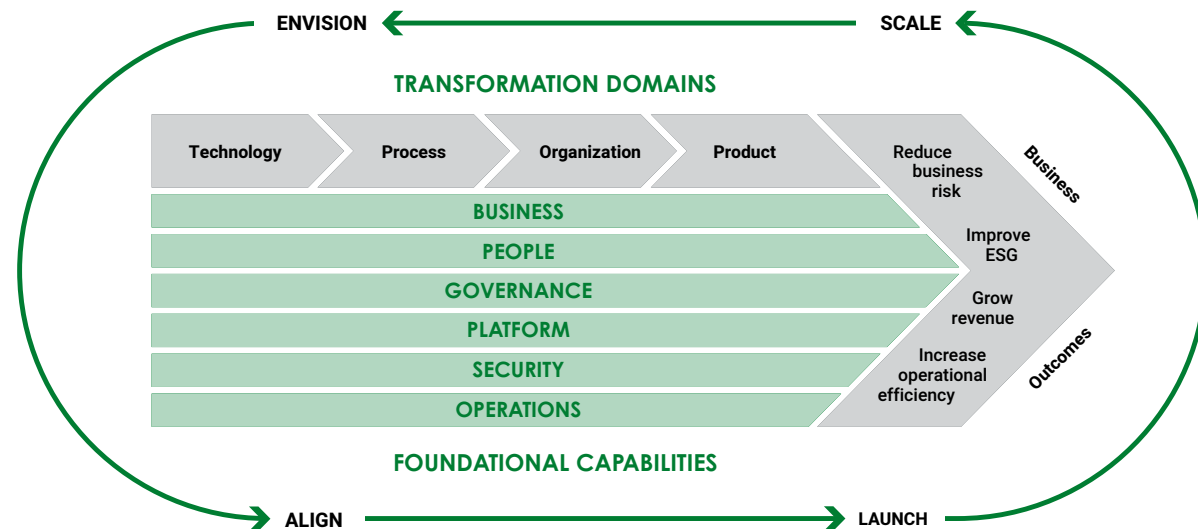
In order to use the flexibility of the public cloud safely, the trick is to define frameworks, or guardrails if you will, within which you remain agile.

Security first with a Cloud Adoption Framework

In order to help you make that shift, today's largest cloud providers (Amazon, Google and Microsoft) developed a Cloud Adoption Framework (CAF), [like this one from Amazon](#). The CAF is a model that covers all topics that can be part of a transformation to the public cloud. They contain a lot of useful advice and guidelines to help change the strategies of an organisation.

Security is a critical flow within this framework, affecting different layers of the organisation. How do you give security the priority it deserves? What should you pay attention to? In short: what is involved in a successful and secure transformation towards the public cloud? In the following chapters, we will discuss layer by layer the key focus points to answer these questions.

Security is a critical flow within this framework, affecting different layers of the organisation.





LAYER 1

Fundamental choices

Although the public cloud offers a high degree of flexibility, you need to make some well-considered decisions in advance; for security reasons and because correction afterwards involves high costs. At this initial stage, for example, it makes no sense to discuss detailed firewall rules, because you can in fact easily adjust this later on in the public cloud.

Reason from a business perspective

As far as we're concerned, decision-making is always based on business objectives, not technology. The IT environment must be designed based on these objectives. This also applies to the security requirements. What are the safety requirements the company must meet? Different rules apply to banks and insurers. They have to comply with strict compliance guidelines compared to, for example, production companies. A clear definition of what you want to achieve with the public cloud should therefore always be the first step.

"Starting with the business" means that more is required of the knowledge level of business managers. The choices they make affect the IT area, but they don't always have sufficient knowledge to foresee the consequences of those choices. Especially in complex environments, in which data flows run through various internal and external networks to provide specific applications with data, IT choices can soon lead to adverse consequences for the working method and the resilience of the organisation as a whole. Continued investment in this knowledge level is therefore vital.

"Starting with the business" means that more is required of the knowledge level of business managers.

Excluding certain regions with a cloud provider is a cost management measure and a security solution in one.

A strong foundation

Some things are difficult and expensive to change at later stages in your cloud migration. Depending on your organisation, this can be achieved in various ways, but we would like to highlight two of these for you, because they are still often ignored in practice.

Active geographic regions

Public cloud environments can be set up across the globe. For example, to be closer to your customers and to reduce latency. Or you implement an environment in a specific region on account of strict local compliance requirements. It is equally important to determine which regions you do or do not use. Excluding certain regions with a cloud provider is a cost management measure and a security solution in one. Nothing can happen in excluded regions and if it does, it's an immediate signal that something isn't right.

Organisational structure of the Cloud

We don't recommend creating a single cloud account for the entire environment. This basically puts all your eggs in one basket and if something does go wrong within that account, you lose it all in an instant. So it's wise to think about your structure. This can take on different forms, depending on your specific needs: per department, per application and even per business model. A project organisation needs a different account structure than a technology supplier.

These matters can be arranged in e.g. the tailor-made **Cloud Landing Zones** by Solvinity, which reduce all available services and endless functions and possibilities into a single manageable whole.

Focus points

- ≡ Make sure that the business and strategic objectives you want to achieve with the public cloud are clear.
- ≡ Map out what knowledge your organisation has internally and then assess whether you should engage an external partner for advice, training or outsourcing.
- ≡ Find out whether your managers have the right knowledge to make security and compliance decisions for the new public cloud environment, among other things.
- ≡ Evaluate in which regions the organisation is active and what the ambitions are with regard to international expansion.
- ≡ Classify the desired cloud activities based on business operations and business objectives and determine the account structure based on this.



LAYER 2

Network framing

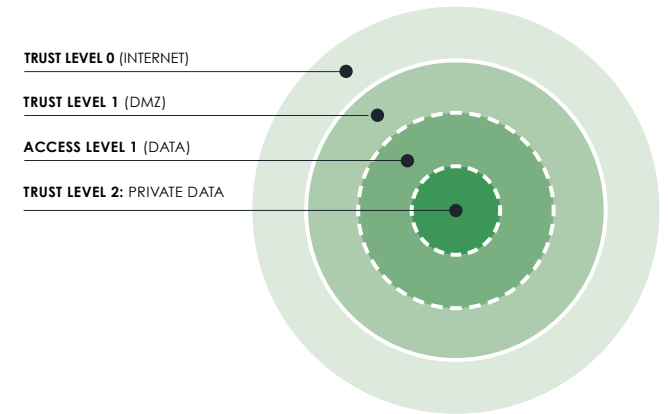
After the fundamental choices have been established, you can build your network on top of that foundation. Solvinity recommends using Zero Trust principles. This means that no one inside or outside the network is trusted by default and that authentication is required at all times from anyone trying to access network components.

Critical network security tools

“Security by Design” principles are important for the set-up.

At Solvinity, this means that all processes, applications and systems under management are continuously checked for possible weaknesses from as early as the design phase. Examples include segmentation and hardening. In the case of **segmentation** your networks are separated. Which parts really need interfaces and which can do without?

Don't set up
networks as 'trusted',
but as 'not trusted unless'.

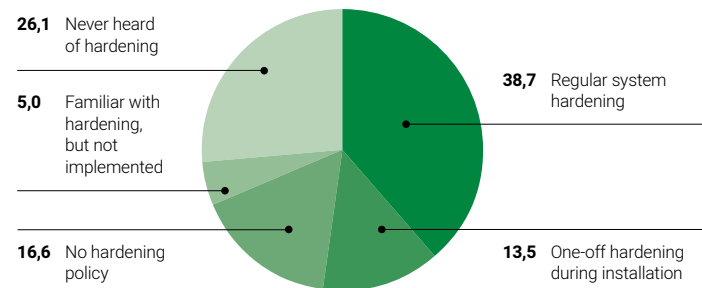


By separating different parts of the infrastructure as much as possible, intruders who break through the first defence do not have direct access to the entire network. Don't set up networks as 'trusted', but as 'not trusted unless'.

Be sure to apply segmentation to your data storage using **Identity & Access Management**: do you provide for a data access policy for everyone, or do you put sensitive data (such as legal documents or intellectual property) in a strictly separated segment that cannot be automatically accessed by any user? Do you apply automated access rights to every file or folder? By formulating the answers to these questions in advance, you limit the impact of unexpected data breaches.

In the public cloud,
the implementation
is not the bulk of
the work, rather setting
policies and making
choices to back these up.

Hardening is a process in which all possible settings within an IT environment are checked to maintain the right balance between functionality and security. And that balance is delicate: a wrong choice in one network segment can have undetected consequences elsewhere. This is often done just once, when building the infrastructure. Or not at all: [according to our own research](#) 40% of IT managers are not familiar with the concept. A serious observation, because we deem hardening a crucial and ongoing process. After all, every change can affect the entire infrastructure. With every upgrade and change, we therefore look at the possible impact on the infrastructure to ensure resilience. Hence we refer to this as **continuous hardening**.



Haste makes waste

In the public cloud, the implementation is not the bulk of the work, rather setting policies and making choices to back these up. This is an example of the necessary change in mentality. Don't take a quick decision, just because you expect the implementation process to take a long time, as that isn't the case in the public cloud. Focus on the policy choices first and make sure you are well informed in advance. Define the environment well, yet at the same time allow for flexibility to experiment, even with new security features. Cloud features are easy to activate and if they don't seem to suit your organisation, they are just as easy to switch off again.

Focus points

- ⚡ Create transparency about access to applications and environments for both internal and external target groups and secure this according to proven principles, such as Security-by-Design.
- ⚡ Specify the conditions under which access to applications or data may be obtained, assuming Zero Trust as much as possible.
- ⚡ Identify your 'crown jewels' and take an extra critical look at access rights and access reasons and the policy for (temporary) access to those critical parts. Include service accounts in that as well.
- ⚡ Map out which frameworks you want to apply to offer your transformation maximum effectiveness without automatically giving everyone complete freedom of movement.



LAYER 3

Security at application level

With a well-designed network infrastructure and Cloud Landing Zones, you have a solid foundation to build actual applications and services. This is where the concepts (Stretched) DevSecOps, shift-left security and Agile Security come into play, as they fulfil an important role in keeping public cloud environments safe.

Shift-left security

DevOps is a trend within application development that bridges the gap between software development and IT management, allowing you to roll out product updates much faster, which are then also more manageable. Yet security is not always a priority when pursuing speed in rolling out updates. That is why a movement called **DevSecOps** has arisen that aims to include security during all phases, from concept to management, as a permanent part of the development process. In this model, developers ensure that the system works as it should, administrators are responsible for reliability and maintenance of the system, and security tests the product against safety standards. This results in **shift-left security**, in which application security is part of the development process from the very outset (the 'left side' of a timeline).

Stretched DevSecOps

Solvinity has developed a collaboration model partly based on these principles that combines outsourcing with rapid software releases.

Stretched DevSecOps aims to deliver new functionality predictably, safely and smoothly, also when IT management is outsourced.

Stretched DevSecOps aims
to deliver new functionality
predictably, safely and smoothly,
also when IT management
is outsourced.

Agile security aligns security testing with development speed by spreading pen tests throughout the year.

This allows teams to determine much earlier in the process whether new releases cause any vulnerabilities and whether service reliability is compromised. The “Stretched” part means that Solvinty’s experts are embedded in our clients’ teams, thereby ensuring that lines are kept as short as possible and that the desired development speed is not compromised. As a result, there are no longer any walls between our organisation and that of the customer, resulting in development speed, improved communication and knowledge transfer. Yet “Stretched” means more than working together and ‘breaking down walls’. Stretched DevSecOps means continuous collaboration, learning and evaluation.

Pen testing and Agile Security

Finally, you need to be sure that the production environments are secure, including after the development and release stage. That’s why at that stage, it makes sense to deploy **pen testing**, which simulates cyber attacks on a system to evaluate its security. However, the frequency of pen tests is usually too low. Pen tests are perhaps performed once or twice a year, while new software updates are rolled out monthly or perhaps even weekly.

Agile Security aligns security testing with development speed by spreading pen tests throughout the year, thus testing where and when changes are made. This way, security remains top-of-mind and an integral part of the process without compromising too much on flexibility or speed, whilst preventing damage to your reputation and unexpected costs afterwards.

Focus points

- ⚡ Evaluate the suitability of your current test model for application assessment and security and identify areas for improvement.
- ⚡ Map out the design and development process and the structuring of applications.
- ⚡ Evaluate the organisation and degree of optimisation between different teams and disciplines.
- ⚡ Understand how and why (important!) audits take place, as well as what is audited, and prepare for this in good time.
- ⚡ Make sure to have a complete picture of communication with and between applications.



LAYER 4

Protection against external threats

The layers discussed above provide for security built up from within. Additional measures must then be added that explicitly target external threats.

Protect, Detect, Respond

Solvinity follows the proven principle of Protect, Detect, Respond, which is reflected in, for example, the [NIST framework](#):

- The **Protect** aspect has already been partly discussed in previous layers. Identity & Access Management allows you to determine which users have access to specific data and applications. Add an additional layer of security at hardware level, by controlling which devices get which levels of access. Finally, implement technologies such as anti-DDoS and anti-ransomware solutions.
- In short, **Detect** means the targeted logging and monitoring of all components and configurations to discover changes or deviations. After all, if someone has penetrated your network, you don't want to wait six months to find out. And although you can conduct an in-depth defence with thorough network segmentation, it is desirable to also monitor for attacks before they succeed. Examples include the central and secure storage of all logs in a totally protected location, which is necessary

anyway for compliance and facilitation of audits, and the use of monitoring solutions such as Advanced Threat Detection. Sandboxing in particular is a powerful tool in this regard. This is a method of activating programs in a completely shielded environment (the sandbox), so that they can be safely monitored there.

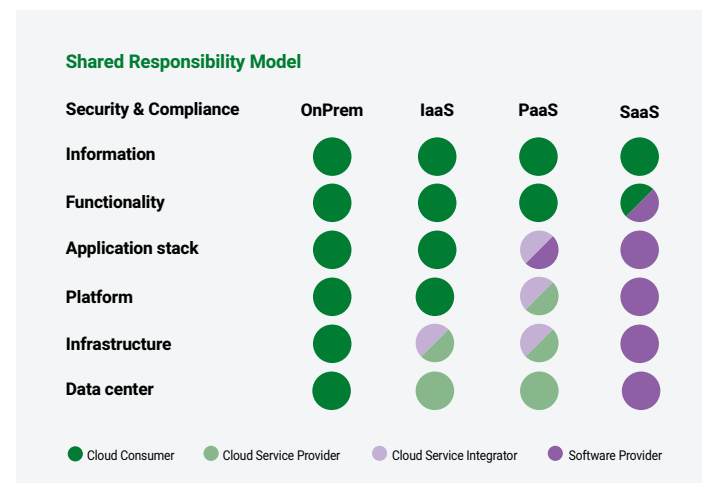
- Finally, the **Respond** phase requires speed and therefore preparation. Have playbooks ready: a list of prepared, preferably automated steps in response to threats. Such a step can be a simple notification, but also the automatic closure of a network. Either way, playbooks allow your teams to respond efficiently and effectively without unnecessary consultation. Also provide for damage-limiting solutions in the context of Disaster Recovery in the unlikely event of an emergency occurring and your IT environment being compromised.

The fact that you can
arrange security per
application or per
environment is precisely
the power of
public cloud.

Prevent one-size-fits-all security

An important caveat is that while the Protect-Detect-Respond principle promotes a holistic approach, within public cloud environments you must utilise all possibilities to maintain flexibility and granularity. The fact that you can arrange security per application or per environment is precisely the power of public cloud. You gain momentum by using the managed services of the Cloud Service Provider. This way, you don't have to cram all applications into a single model and you can outline your policy per type of application and/or environment.

A proper understanding of the **Shared Responsibility** model is useful in this respect. This outlines the responsibility of security in the public cloud and how it is divided between the user and cloud provider. In short, users are responsible for safety within the cloud (including their data), whereas cloud providers are responsible for security of the cloud systems, compute systems and storage systems and the networks that support the public cloud. In other words: the infrastructure may be safe and compliant, but that does not automatically mean the applications running on it are as well.



Focus points

- ≡ Know where and how the Shared Responsibility Model impacts the security and compliance status of your environment.
- ≡ Determine how and which threats to respond to.
- ≡ Provide insight into which emergency plans exist within your organisation or draw up these plans if not yet in place.
- ≡ Find out how and how often these plans are tested.
- ≡ Evaluate which technical measures have already been taken against external threats and supplement these where necessary.

The human factor

So far, we have stayed close to the technology. Yet security also depends on the human factor. This deserves special attention within every organisation, because [a large part of successful cyber attacks](#) are caused by human intervention.

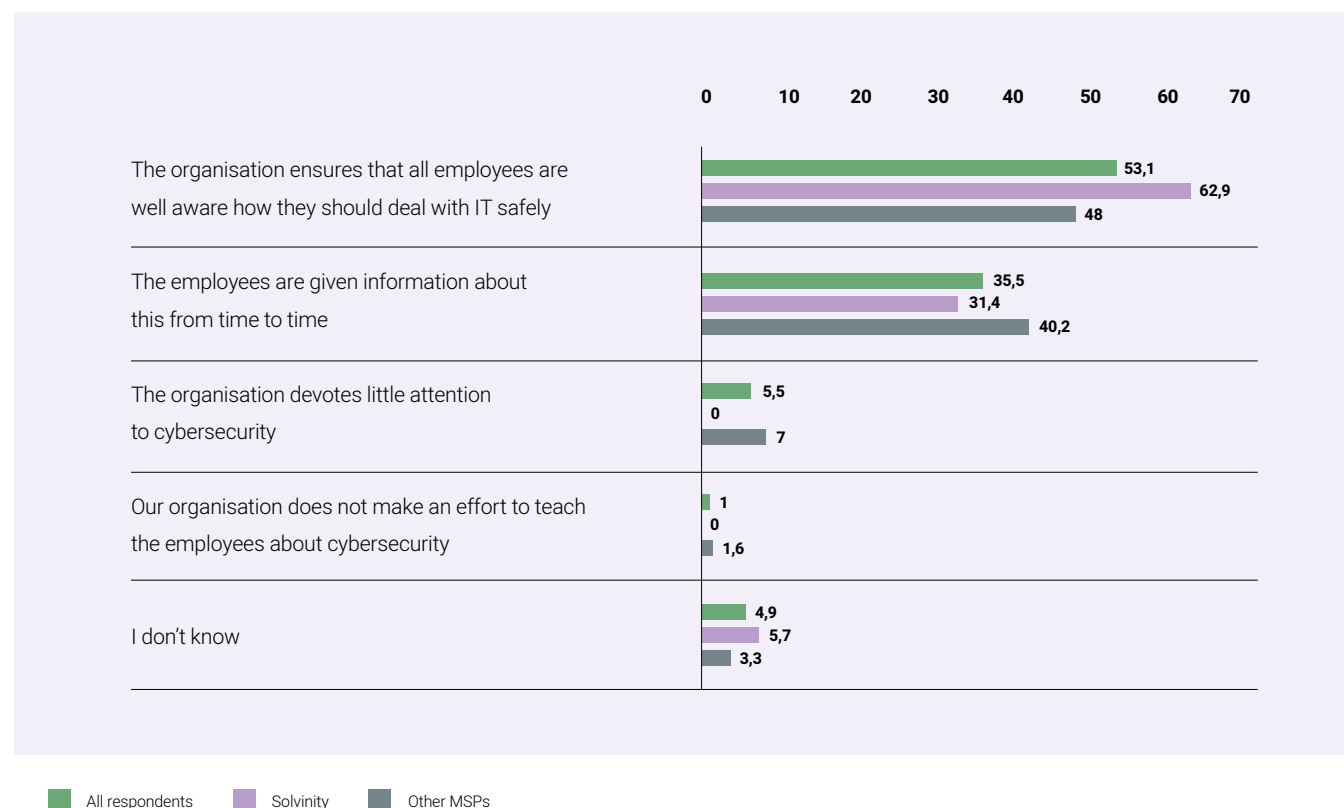
Creating awareness

First of all, **security awareness** among *all* employees is a crucial part of any security program. [48% of organisations](#) that manage their own IT pay insufficient attention to this, while all employees should know how to work securely in the public cloud. This means that they must be aware of the risks and know what to do if something does go wrong. Therefore, invest in course programmes and inform your employees through **training sessions**.

Furthermore, periodically test the knowledge and 'state of readiness' within the organisation with, for example, **phishing tests**, where you try to secretly obtain personal data via e-mail. Numerous security awareness programmes are available in which employees are continuously and creatively kept on their toes. Solvinty offers **tailor-made programmes** which are made up of various video training courses, games, quizzes and test modules.

48% of organisations that manage their own IT pay insufficient attention to this, while all employees should know how to work securely in the public cloud.

Every innovation within the public cloud can potentially save you money or leave you out of pocket due to means chosen previously.



Knowledge sharing

Secondly, it is important to keep the security knowledge of your IT employees up to date through ongoing **training**. The public cloud world is changing fast, but the threat landscape is changing even faster. Keeping knowledge up to date is essential from a security perspective, but also from a cost perspective: every innovation within the public cloud can potentially save you money or leave

you out of pocket due to means chosen previously. Therefore ensure you continuously invest in knowledge, as this allows you to think strategically about the choices to be made. This also shares common ground with subject of compliance: the right knowledge and skills are required to meet the strict standards of compliance certifications.



Of course, given the complexity of the public cloud, it is not always necessary or even possible to have all the necessary expertise. In that case, the required level of knowledge can mean that your IT teams are able to identify potential threats in a timely manner, so they can quickly engage external expertise. At Solvinity, for example, we deem compliance a critical part of our services and we ensure standards are safeguarded at all times. Due to this attention to compliance, we are the only party in the Netherlands to provide SOC 1 and 2 reports for not only our entire private cloud environment, but also the management environment of the Azure public cloud.

Focus points

- ⚡ Evaluate whether the organisational culture is ready for the transformation to public cloud.
- ⚡ Know which employees and departments will be using which new services.
- ⚡ Determine whether you want people to obtain a certain certification before they take on a leadership role in a transformation.
- ⚡ Map out what you need to do and learn as an organisation to properly manage information security and whether the necessary training is available.
- ⚡ Check whether all internal processes, monitoring, etc. are adequate and up to date for the public cloud.

Every security evaluation
is by definition a
snapshot and should
therefore be performed
periodically and
preferably automatically.

Continuous guarantee

Securing a public cloud environment is not a one-off task. Public cloud is ideal for innovation. Not only the applications of your organisation are constantly being developed; the underlying cloud technologies too are continuously improved. In addition, cyber criminals are not resting on their laurels either. Their attack methods are becoming increasingly sophisticated. All this means that every security evaluation is by definition a snapshot and should therefore be performed periodically and preferably automatically.

The importance of periodic evaluations

Important tools in your armoury are the **Well-Architected Frameworks** developed by [Google](#), [Microsoft](#) and [Amazon](#) for their respective cloud services. These describe the main best practices in concept, design and architecture of public cloud environments, and help you understand the pros and cons of certain choices. Such a framework is therefore a useful tool for evaluating your cloud environment based on current standards and best practices. By periodically completing an assessment based on a Well-Architected Framework, you can more effectively identify new security risks and mitigate them more efficiently.

Judging your own choices can be difficult. Solvinity can support you in this through the Cloud Architecture Assessment. As part of this evaluation process, we help you take a look in the mirror and guide

you in the assessment of your cloud architecture. We ask questions that make you think and that help you strengthen your cloud architecture.

The best lessons are learned in practice

Even a [Cloud Architecture Assessment](#) remains a theoretical story to some extent. If you really want to know if you are safe, then [Red Teaming](#) can provide insight. Whereas security teams know during a pen test that it is taking place and can prepare for it, Red Teaming surprises them. Consequently, they will treat the test as a real attack, which can provide a more complete picture of security, especially in terms of detection and response capabilities. The experts at [Securify, our strategic partner](#), will explore all possible attack vectors, including the (access) security of your physical office.

By periodically deploying various assessment methods, you are more often and better informed about the state of security of your cloud environment, and you are able to identify and resolve gaps in your security more quickly.

The best partner for a secure public cloud environment is one with experience and a background in security, privacy and compliance.

Conclusion

Setting up a well-secured public cloud environment is easier said than done. It requires strategic choices, good preparation and a structured approach. Use all the tools at your disposal. By laying down a solid foundation from the ground up using a Cloud Architecture Framework, you will be well-equipped to protect your organisation against threats with Protect-Detect-Response methods. No organisation should shy away from any method or tool that logically fits within the needs and available capabilities. And that completes the circle.

As we established at the beginning of this white paper, it is not always possible (or desirable) to bring all necessary expertise in-house. In that case, a Trusted Cloud Provider is the way forward. A partner who can support you throughout the entire process from conceptualisation to periodic evaluation and at all layers discussed in this white paper.

Of course, not all partners are equal. The best partner for a secure public cloud environment is one with experience and a background in security, privacy and compliance. But just as important is that this partner works transparently with you, so that you can take full advantage of the knowledge this partner brings. And finally, the culture fit is important. After all, it is better to work together with a group of professionals that you hit it off with.

Solvinity offers a unique portfolio of security services in the Netherlands, not only for the design and management of your cloud environment, but also for ongoing retrospective testing and security awareness programmes. After reading this white paper, are you curious whether you will click with Solvinity? We look forward to talking to you some more!





You may also be interested in:

≡ White papers

[Integrated Delivery](#)

[Security by Design](#)

≡ Multimedia

[Control over public cloud security \(Dutch\)](#)

[Cloud native application development \(Dutch\)](#)

≡ Blogs

[Make the right strategic choices with a cloud architecture assessment](#)

[Landing zones, the best starting point for the public cloud](#)

[From account to application safe at all times in the cloud](#)

[7 critical success factors for a safe and compliant cloud first strategy](#)








[A safe transition to the public cloud, what should you keep in mind?](#)

[Speed, security and smooth collaboration with Stretched DevSecOps](#)

[Shift-left security with Stretched DevSecOps](#)



With secure managed IT services Solvinity advises and supports organisations with
 high security requirements in their digital transformation.

	Managed Cloud Outsourcing	Security & Compliance Lango Workspace	Service Integration Application Services
	Solvinity has distinguished itself in the field of cybersecurity with a special portfolio of security services and solutions and offers, with a majority share in Security , additional services for pentestig, red teaming and agile security.		
	Certifications according to (inter)national standards such as ISO 27001, ISO 14001, ISO 9001 and PCI DSS. The first Managed Service Provider in the Netherlands with SOC 1 & 2 reports for the management environment of not just the private, but also the Azure cloud.		
	Solvinity provides services to (national)government, municipalities and leading organisations in financial and business services, like the Ministry of Justice and Safety, the Dutch Police, TransLink (OV chipcard), ING and ONVZ.		
 350 staff members	 2021: turnover 59 mln	 Amsterdam, Assen Amersfoort, Den Bosch	
