



INSIGHTS PAPER

Impact on your brand & business

A man with short dark hair, wearing a dark denim jacket, blue jeans, and black Converse sneakers, is sitting on a set of light-colored wooden steps. He is looking at a laptop screen which displays a web application with various charts and data. The background shows a blue circular rug on a grey floor.

7 best practices to maximise your cloud environment

Edition - Cloud, data & integration



An effective IT architecture is not a luxury, but a necessity, in a world where getting the very best out of digital opportunities is often all that stands between success and failure.

A well-designed cloud environment will help your organisation to stay innovative and agile, but that is not always easy due to the associated knowledge, technical complexity, cost considerations, security and compliance requirements, etc.

In this Insights Paper, we'll discuss 7 best practices that you should follow so you can take full advantage of the opportunities offered by the cloud.

Contents

The evolution of the cloud: from hardware-focus to software-centric thinking	4
7 best practices for leveraging the cloud	7
1. Maintain a strategic focus on data	8
2. Take a proactive approach to cost control	9
3. Manage security & compliance	12
4. Support the self-servicing developer	13
5. Adopt industry standards	15
6. Invest in knowledge building and sharing	17
7. Design for resilience	19
iO's pillars for effective cloud use	20
Checklist: How cloud mature is your organisation?	21

The evolution of the cloud: from hardware-focus to software-centric thinking

IaaS

The first generation of cloud

Larger organisations faced the challenge of keeping their own physical IT infrastructure up to date. This was underpinned by long purchase processes with high costs for servers, storage space, data centres and network equipment – both in terms of investment, management and maintenance.

With the rise of **Infrastructure as a Service (IaaS)**, ownership and maintenance of IT hardware is no longer all on the user. Instead, the IaaS provider took **responsibility** for managing servers, hardware, and data storage.

With IaaS, there is no need for substantial **upfront investments** in hardware, because it has been replaced with a subscription or **rental model** for the virtual machines, storage and networks. Organisations can respond quickly to changing needs and only have to pay monthly costs based on actual usage.

PaaS

The second generation of cloud

Companies rapidly became accustomed to cloud-native practices: where everything starts with the cloud. This also brought new expectations: the ability **to develop and deploy business applications faster**. And above all, that these applications dynamically **scale** with the number of users.

Instead of developers having to set up and manage the entire underlying IT infrastructure when building applications, with **Platform as a Service (PaaS)**, the cloud provider takes care of the allocation of computing power, scaling, and management services.

Developers were free to focus on code, not on the infrastructure (security settings, server management, etc.). This drastically accelerated the time-to-market of new applications.



SaaS/iPaas

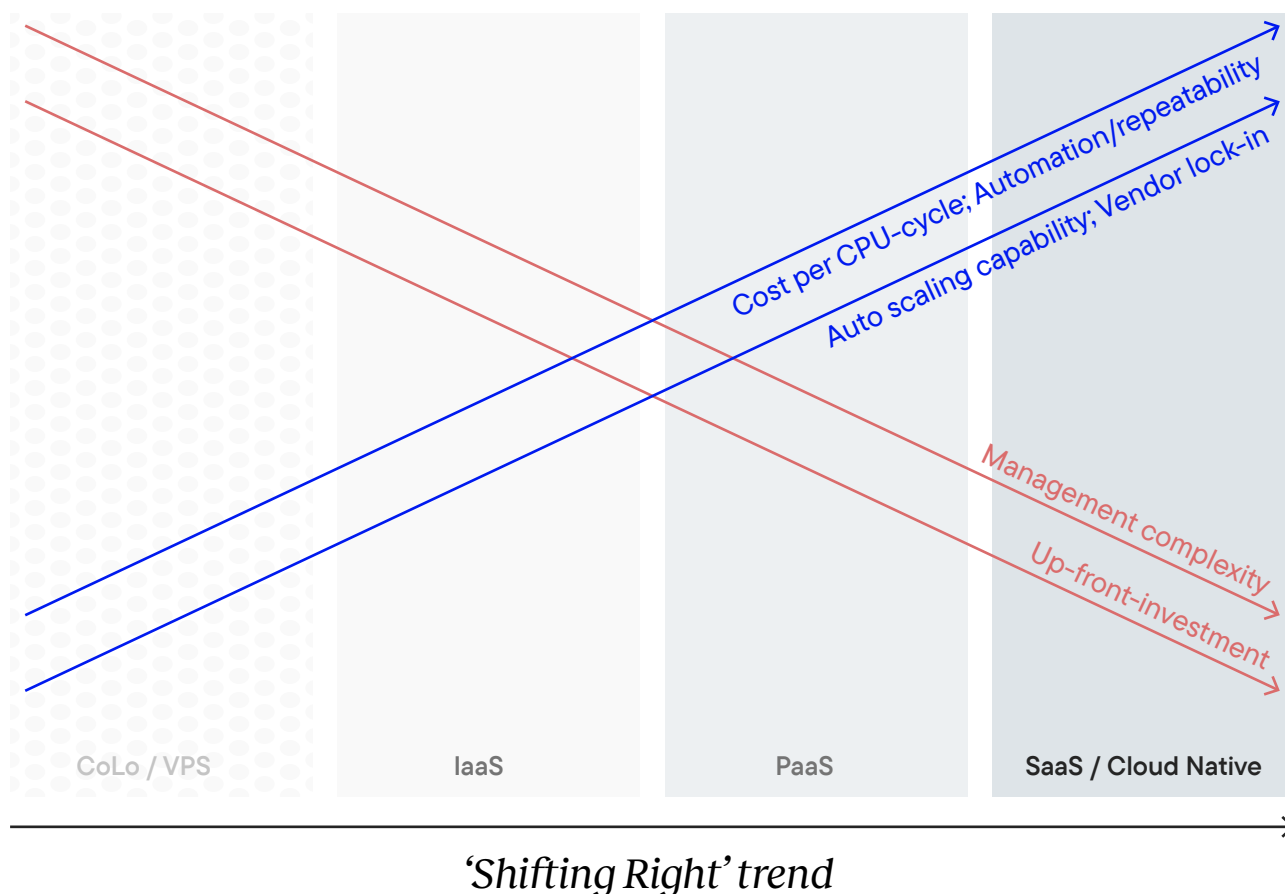
The last generation of cloud

As more and more business processes digitised, the need for **off-the-shelf software solutions** that could be easily deployed grew.

Software as a Service (SaaS) allows organisations to use services such as CRM systems (Salesforce) or productivity tools (Microsoft 365) directly without worrying about installation, maintenance, updates, security, and infrastructure.

The growth of SaaS applications within organisations brought a new challenge: how do you ensure that all these different systems and applications communicate effectively with each other?

Integration Platform as a Service (iPaas) offers a solution for this by connecting cloud applications and on-premises systems: it helps organisations to make their various IT systems work together seamlessly.



Less freedom but more possibilities

There has been an undeniable shift in the way organisations organise their IT landscapes over the past two decades.

Companies are shifting to the right on the Cloud Evolution Model described above, opting for managed solutions (SaaS) that take management responsibilities out of their hands and offer more support with security and scalability.

While this shift to the right also means that organisations have **less freedom** in infrastructure configuration, it offers significant **benefits**. Think of quicker time-to-market, less time spent on managing IT, etc. This allows companies to focus on their core business instead of investing time and resources into the management of complex IT systems.

However, **effective cloud implementation and use isn't automatic**. It requires research, knowledge and carefully considered choices. In the following chapters, we discuss 7 important aspects of smart and effective cloud use.





7 best practices for effective use of the cloud

1. Maintain a strategic focus on data

Are you ready to unleash your data's full potential?

Contemporary cloud solutions such as [AWS](#), [Azure](#) and [Google Cloud](#) offer unprecedented capabilities to collect, store, transform, and analyse data at scale. They offer advanced services such as serverless data warehouses or machine learning platforms.

From centralised...

However, not all data is equally relevant and 'insatiable data gathering' does not align with recent European legislation. Organisations need to think carefully about what they want to measure, store, and of course when, and how. For years, many organisations have worked with a single database for all data. In practice, we often see that this centralised approach creates too much data flow and demands a lot of handling. And what's more, a centralised data team that manages such a platform doesn't necessarily have enough domain knowledge to turn all that data into worthwhile, usable insights. Data-collection does not equal data-driven.

... to decentralised.

With data mesh, responsibility for structuring that data no longer lies with the central team. Now different product teams manage the data that is relevant to their part of the customer journey or a customer application. In fact, data is not held centrally. It is held across the organisation but with connections that facilitate communication between the different locations. This allows the different data sources and methodologies that collect data to coexist, but establishing appropriate lines of communication that allows the data to flow from one vessel to another is essential.

As a result, data and intelligence, which was previously exclusively an IT matter, is now a shared responsibility across the business.

Cloud providers deliver the foundations required for a data mesh vision; you can store data decentrally at very manageable costs, design data integrations or access it easily using APIs. In 2025, serverless data warehouses are a cost-efficient way to bring the extracted data together from the organisation via meshes, after which smart analyses make you truly data-driven.



In a nutshell

The cloud offers many possibilities, but the success of your cloud strategy depends on the way your organisation handles data. Be truly data-driven by balancing the power of the cloud with effective data management.

2. Take a proactive approach to cost control

How does the use of cloud services translate into costs for your organisation, and how do you control those costs?

That is more difficult to predict (and budget for) the further you move to the right side of the Cloud Evolution Model.

Up-front costs are more difficult to predict

Unlike traditional IT infrastructures (where large investments are often made upfront), **cloud costs increase with usage**. This offers flexibility, because the costs adjust based on the success of your business: the more your business grows, the more licenses, user numbers, computing power, storage and services you purchase, the more you pay.

In principle, you could say that your costs become more predictable because they increase with use, but in the long term, the costs are still difficult to estimate in advance. *Do you know how successful your business will be?*

Insight: the basis of everything

If you don't have a good cost control strategy, you run the risk of rapidly rising costs that can be difficult to control. It's wise to have a clear understanding of what your costs will look at from the start.

Make smart use of the tools offered by cloud providers. They provide very detailed insights into costs through tagging and resource groups. This enables you to place the responsibility for specific costs in the right place in your organisation, following to the 'you run it, you pay it' principle.

And it may sound obvious, but: keep a close eye on your invoices. Monitor your accounts periodically to avoid surprises and to intervene quickly in the event of deviations.



Dependence on a cloud provider

Be mindful of vendor lock-in when working with a cloud provider. As a business relies more on SaaS and iPaaS solutions, the reliance on the chosen vendor(s) increases, making it difficult and costly to switch to another cloud provider.

And what about the Multi Cloud approach?

Sometimes **Multi Cloud** (purchasing services from different cloud providers) is suggested as a solution to avoid dependence on one provider. In practice, this approach rarely delivers what is expected of it. Adapting your entire infrastructure to work with all cloud providers is often much more expensive and outweighs the benefits of standardising with one cloud platform.

Vendor lock-in plan

At iO, we see **some level of commitment to a cloud provider** as inevitable. It is inherent to working in the cloud.

Therefore, accept a vendor lock-in to a certain extent, but make sure that you choose standards and components that are mature and widely supported in the market. This minimises the risk of being stuck with technologies that become obsolete and helps to minimise future switching costs.



In a nutshell

By taking a proactive approach to cost control, you can identify inefficiencies and avoid paying more than necessary. This not only helps with controlling expenses, but also ensures that your budgets remain realistic and your financial planning is in order. Have you got the right tools and processes in place to effectively manage and optimise your cloud costs?



“In 2024 alone, AWS and Azure released more than five specialist cost analysis tools and dashboards. Fortunately, they are also becoming more coherent and connected to each other, making them usable for more engineers and finance experts. Give them a try: you’ll earn your investment back in a few months.”



FRISO GEERLINGS
Technology Director

3. Ensure security & compliance

How do you find the perfect balance between essential safety and security with costs?

Organisations are entrusting more work and data to the cloud. But the more data that is moved to the cloud, the greater the responsibility to handle it carefully. On the one hand because of cyber threats, on the other because of laws and regulations.

Security threats

Modern cyber threats, such as data breaches, are so complex that often they cannot be effectively addressed without cloud services. The level of security required for this is almost impossible to achieve today.

Cloud providers are investing heavily in this, with teams of experts working 24/7 to identify and combat risks and threats. They have the scale and expertise to provide advanced protection against a wide range of cyberattacks.

Evaluate the costs and benefits of security options

With many cloud providers, an extra security feature is often just a matter of ticking a box. However, advanced security features such as web application firewalls or cloud-based monitoring tools can be pricey. **So, be aware of the cost of security features and be deliberate about their application.**

For example, when your organisation has a certain social impact or when you work with sensitive data such as medical information, children's data or financial data. Not all security measures are equally relevant or cost-effective for every organisation.

Compliance requirements

Nowadays, it is almost impossible to meet strict compliance standards such as PCI DSS, ISO 27001 and NEN 7510 without a cloud provider. For example, do you want to set up an ISO 27001-compliant infrastructure in-house? That gets more expensive and labour-intensive than using [AWS](#), [Azure](#), [Google Cloud](#) or other large players very quickly. This includes not only the costs for implementation and maintenance, but also the personnel costs to keep everything up-to-date and secure over the long term.

Who is responsible for what?

Make sure you understand where the responsibility for security and data protection lies. Is it with the cloud provider or is it the responsibility of your organisation and administrators. Understanding the 'shared responsibility model' can be a challenge at first, but that is precisely a point where you have to invest in order to get the entire chain in order.

In a nutshell

Conduct a thorough risk analysis to determine which security features are essential for your specific use case. Not every organisation needs the highest level of DDoS protection.

4. Support the self-servicing developer

How do you use the freedom that comes with the cloud, without losing sight of frameworks, boundaries and costs?

The development process can often be frustrating when internal processes are slow. Being **limited to slow iterations** or restricted by **complex management and maintenance tasks** can also slow down innovation and the development process.

Ideally, you want developers to have freedom and be able to experiment and iterate quickly, without being hindered by long wait times or complex processes.

The cloud offers great solutions for these issues.

The 'self-servicing developer'

Within the cloud, a developer has the ability to set up, manage, and maintain **the necessary infrastructure and resources for their projects themselves** – without the need for IT teams.

For example, the self-servicing developer can build prototypes and iterate quickly, or test scaling infrastructure during peak periods. This significantly speeds up the development process compared to traditional on-premise infrastructures. This is particularly valuable for large organisations, with management hierarchies and structures that lack agility.



How to give developers freedom and responsibility:

1. Cost awareness

Self-servicing developer freedom also comes with risks: developers don't just need to know how to build applications, but also how to run them efficiently in the cloud. They need to understand how their choices impact costs, something that developers are not always aware of. Without regard for costs, resource utilisation can easily get out of hand.

2. Knowledge development

All developers should be trained to have the same **level of knowledge**, so that they can make informed choices. The more responsibility they have, the more important this training becomes. Cloud providers respond to this proactively by offering a whole range of training courses and workshops.

3. Controllers

We also strongly recommend building in extensive checks and balances. Cloud providers provide policies that allow IT/Infra experts to set frameworks for developers, such as enforcing security levels, resource logging, and budget limits. These policies, along with automated controls such as feedback loops, ensure that security, compliance, and costs stay manageable. For example, you can warn of unused resources or automatically shut down inactive servers.

4. Infrastructure as Code (IaC)

Freedom to experiment is important, but as soon as a project moves towards acceptance or production, there needs to be more structure. The principle of Infrastructure as Code (IaC) enters the picture here. IaC ensures consistency and repeatability across the project by managing infrastructure as software code. Tools to implement IaC are Bicep (Azure), CloudFormation (AWS) and Terraform (cloud-agnostic). With the right application, IaC can help facilitate an environment where developers have the freedom to innovate, while IT/Infra/Cloud experts maintain an overview and take control.

In a nutshell

The self-servicing developer is both a provision of the cloud and a strategic choice: it offers enormous advantages in terms of speed, flexibility and innovation but also requires careful implementation, clear frameworks and investment in training.

5. Adopt industry standards

How can you stop doing repetitive tasks and use trustworthy standards instead?

Cloud providers such as [AWS](#) en [Azure](#) offer **standardised architectures, security protocols, and services** based on industry best practices. They have been developed by teams of experts and offer your organisation a solid, secure and scalable foundation to work in and can be used immediately. Think of frameworks such as Well Architected, standards such as OAuth and fixed methods of role-based access control works.

As an organisation, it is important to ask yourself:

‘Do we have the time, people, and resources to achieve the same high standard of security and scalability by building our architecture ourselves? And should this even be a question at all, or does it distract from our core activities?’



Unleash the full potential of the cloud with standardisation

Through deliberate standardisation, organisations can realise the full potential of the cloud and reduce exposure to risk. Aspects such as security, integration and scalability are extremely complex and require highly **specialised knowledge**. Many companies think they have this knowledge in-house and can keep it up-to-date. This is not feasible for most organisations.

Don't fight the system

At iO, we sometimes meet people that think that standard cloud solutions are not sufficient. Some feel the urge to deviate from the services. When you encounter this ask yourself the following question:

Is your use case really so unique that the needs cannot be achieved with the standard?

We recommend don't fight the system. Your situation is probably not as unique as you might think. Only deviate in exceptional situations, such as:

- When working with highly specialised technology
- In a niche domain where existing solutions fall short.
- If you need to develop innovative technical applications that don't yet exist.

In a nutshell

Use the standard solutions that are offered by cloud providers such as [AWS](#) and [Azure](#) when possible. So that you can harness the full power of the cloud and focus on growth instead of technical complexity.

However, this requires in-depth expertise and a good understanding of the additional costs and risks.

In many cases, it is wise to **adapt your processes to the standard** instead of the other way around.

It is better to become a little **less unique** so that you can use the standards. This makes it easier to scale with developments in the cloud, keep your IT landscape up-to-date and apply new developments (such as AI) quickly.



6. Invest in knowledge building and sharing

How do you make the best use of available cloud knowledge?

The technology behind the cloud is evolving rapidly. Think of newer and faster AI models, super-fast chips for network traffic, extra layers of security against cyber-attacks and possibilities to link a lot of customer data with each other. These changes make it difficult for many organisations to keep up.

Due to enormous amounts of information, many organisations can't see the wood for the trees, and reliable good cloud-skilled professionals are not exactly plentiful and the expertise that is available often stays within specific teams or individuals.

Cloud providers stimulate knowledge building

In recent years, the **provision of information and knowledge sharing** from the major cloud providers has improved dramatically. They share a lot of valuable information and best practices that you can use. Documentation has been much more qualitative in recent years and now there are extensive guidelines available with clear dos and don'ts.

Using this knowledge means you don't have to figure everything out yourself and you can learn from other people's mistakes. This isn't just good for your technical teams; it also ensures a **'first time right' cloud implementation**.

Invest structurally in knowledge:

- Make an annual **Training budget** available for cloud certification. AWS offers a wide range of certificates, as does Azure. Cloud certification is not expensive in itself, it's the investment of your employees' time that is expensive. However, this is an investment that pays off quickly: certified employees are better able to optimise cloud services and help your organisation to meet certain compliance requirements.
- Disseminate knowledge within the organisation, for example by organising **knowledge sessions or workshops**.
- Establish your own standards or best practices in a **wiki or intranet** (SharePoint, Confluence, etc.).
- And above all: keep a close eye on your favourite cloud provider's information flow. They regularly organise **events** and **workshops** that offer relevant insights.

In a nutshell

In cloud environments, knowledge building and sharing is often underestimated. Many companies want to be well informed, but do not invest in it structurally and don't make use of available knowledge. Building cloud knowledge within your organisation is just as important as sharing it, because your team's collective cloud knowledge is a defining factor for your success when it comes to getting the most out of your cloud environment.



“Extensive cloud knowledge within your teams is the best way to guarantee that you can deploy cloud solutions in the most efficient, secure and cost-effective way.”



ERIK POST
Technology Director

7. Design for resilience

How do you prevent small disruptions from having wider impacts?

The failure of a server in one region can quickly lead to the complete failure of a service, especially when an organisation operates across multiple regions. Or part of a website breaks down, and then the entire site no longer works. Downtime leads directly to loss of revenue, data loss and in the longer term to loss of trust among customers.

By building resilience into your systems, you prevent a small outage from bringing your entire shift to a standstill, especially (but not only) if you are active across a larger region.

How to make your cloud environment resilient

Cloud environments offer a lot of automatic protection, but to build resilience, you need to design your cloud infrastructure strategically. This goes beyond technical measures; It is also an organisational investment.

In a nutshell

Cloud environments offer a lot of automatic protection, but you also need to design your systems to get the most out of it. If you have a resilient IT infrastructure, it will recover quickly from failures with minimum downtime.

Applying the appropriate principles and measures will ensure that your systems are designed to continue to work even if there are problems:

→ **Chaos engineering**

Wonder “What if this component fails?” The ‘chaos engineering’ principle helps you to identify and address potential weaknesses in your architecture. Also take time to test this from time to time, especially in a test environment. Netflix has their famous ‘chaos monkey’ that pushes random applications into failure to test resilience. That could seem extreme, but it is an interesting thought experiment to apply to your own cloud environment.

→ **Stateless architecture**

Design as much of your cloud environment as an application without a ‘state’ as you can: everything you need to keep for a longer period should be kept on cloud-native storage solutions in managed databases or buckets so that a new server or region can take over a failing environment easily.

→ **Event-based**

Event-based work: applications respond to each other using queues and messages, so that in the event of a (temporary) outage, things just wait and then continue running.

→ **Serverless**

Where possible, use cloud-native serverless techniques such as Lambda or Functions; these are automatically distributed by cloud providers over multiple regions so that your application continues to run, even in the event of disruptions in part of the infrastructure.

iO's pillars for effective cloud use

1. Data

Implement a data mesh approach for efficient and decentralised data management.

2. Cost control

Make sure you have a clear understanding of how your costs are built up from the start and make smart use of the tools that cloud providers offer.

3. Security & compliance

Conduct a thorough risk analysis to determine which security features are essential and weigh costs against benefits.

4. Self-servicing developer

Give developers a lot of freedom and responsibility within clear frameworks and control mechanisms.

5. Industry standards

Take advantage of the cloud providers' standard solutions and only deviate in truly exceptional use cases.

6. Knowledge building & sharing

Invest structurally in cloud knowledge and encourage active knowledge sharing to unlock the full potential of your cloud environment.

7. Resilience

Implement both technical and organisational measures to prevent downtime.



Checklist

How cloud mature is your organisation?

1. Do you have a clear view and control over your cloud spending? Are these regularly monitored and optimised if necessary?
2. Have you performed a risk analysis to determine which security features are essential for your organisation and which are not?
3. Is cloud knowledge being actively shared within your organisation through training, documentation, and internal knowledge bases?
4. Are you following the best practices as recommended by the cloud provider, and applying them consistently across your cloud environment?
5. Do you have insight into which data you need or want to store, for how long and where, and have you selected the right cloud platforms and components?
6. Can your development teams set up, manage, and maintain the necessary infrastructure and resources on their own?
7. Do you regularly test your cloud infrastructure to ensure it can withstand outages, unexpected surges and security incidents?

The more elements you have successfully implemented, the higher your cloud maturity level. and the greater the strategic benefits you will get from your cloud infrastructure.

At iO, we make your IT, data and marketing infrastructure scalable and integrate it with the right cloud partnerships and data set-ups.

WORLDLINE 

 brussels
airport

 NN

APPO 

Basispoort 

 FAVORITE
GIFTS

EindhovenAirport 

 Denksport

 Efteling

 Eneco



Why iO?

Technology-independent

Our flexible approach to technology means that we always deliver tailor-made solutions that perfectly match your wishes and needs, rather than relying on generic solutions.

Whether it's Azure, AWS, private clouds, or the right AI models, we prioritise what best fits your goals for optimal performance, scalability, and security.

End-to-end responsibility

We take full responsibility for the solutions we provide. We don't just make the technology and data available, but we also make sure that they deliver the experiences they were created for. From set-up and configuration to monitoring and 24/7 support.

A unique blend of expertise

We combine industry knowledge, marketing expertise, digital skills, and technological know-how to deliver tailored insights and solutions.

By understanding your business goals, we can inspire and offer the right support.

[Get to know us](#)



About iO

iO is a *blended agency*. We blend marketing, technology and creativity because we believe that creating the ultimate customer experience requires a blend of these different skills to make an impact on our clients' brand and business.

With our solutions, we aim for experiences that matter:

Digital platforms →

Brand, Business & Experience Design →

Marketing Programs & Campaigns →

Creation & Content Production →

Cloud, Data & Integration →

Transformation & Consulting →

Experience is
everything

Feel free to reach out:

business@iodigital.com

iodigital.com

