nixu cybersecurity.

Your *to do* list for a secure cloud

– no more learning the hard way

WHITEPAPER

Contents

Executive summary

Companies and organizations worldwide are talking about cloud transformation. The maturity level varies: some companies are planning the transformation, most are in the middle of it, and the forerunners have already transferred all operations and storages fully to the cloud.

The cloud offers many benefits to support modern digital business, such as scalable and a fast platform for testing new apps, IT cost savings, modern workplace tools and flexibility. However, the main concern in cloud transformation projects is cybersecurity. We see that the most critical challenges among cloud transformation projects are related to these aspects:

1. **Lack of visibility.** The same thing that makes the cloud so easy – no need to worry about the underlying infrastructure – decreases visibility to network architecture and traditional monitoring methods may not apply. It can be unclear how service providers handle your data and sometimes security is not involved early enough in cloud transformation projects.
2. **No policy or old policy.** The rush to the cloud has been so hasty that proper security policies have not been set up for cloud environments. If there is a policy in place, it quickly becomes outdated due to the rapid change of cloud security features.

3. **Bad IAM.** Flaws in Identity and Access Management (IAM) lead to lax permissions, untimely de-activation of accounts and security gaps. This problem is current also on the premises, but in the cloud the consequences accumulate.
4. **No time to study the cloud regularly.** People are encouraged to be self-directed, but there's a lot to take in, even for a cybersecurity enthusiast. New features are introduced constantly, while others become obsolete.

Some risks are more critical than others, but all in all, cloud services are not risk-free. Luckily, there's a lot you can do to minimize your risks and take control of your cloud. **Here's our to do list for a secure cloud:**

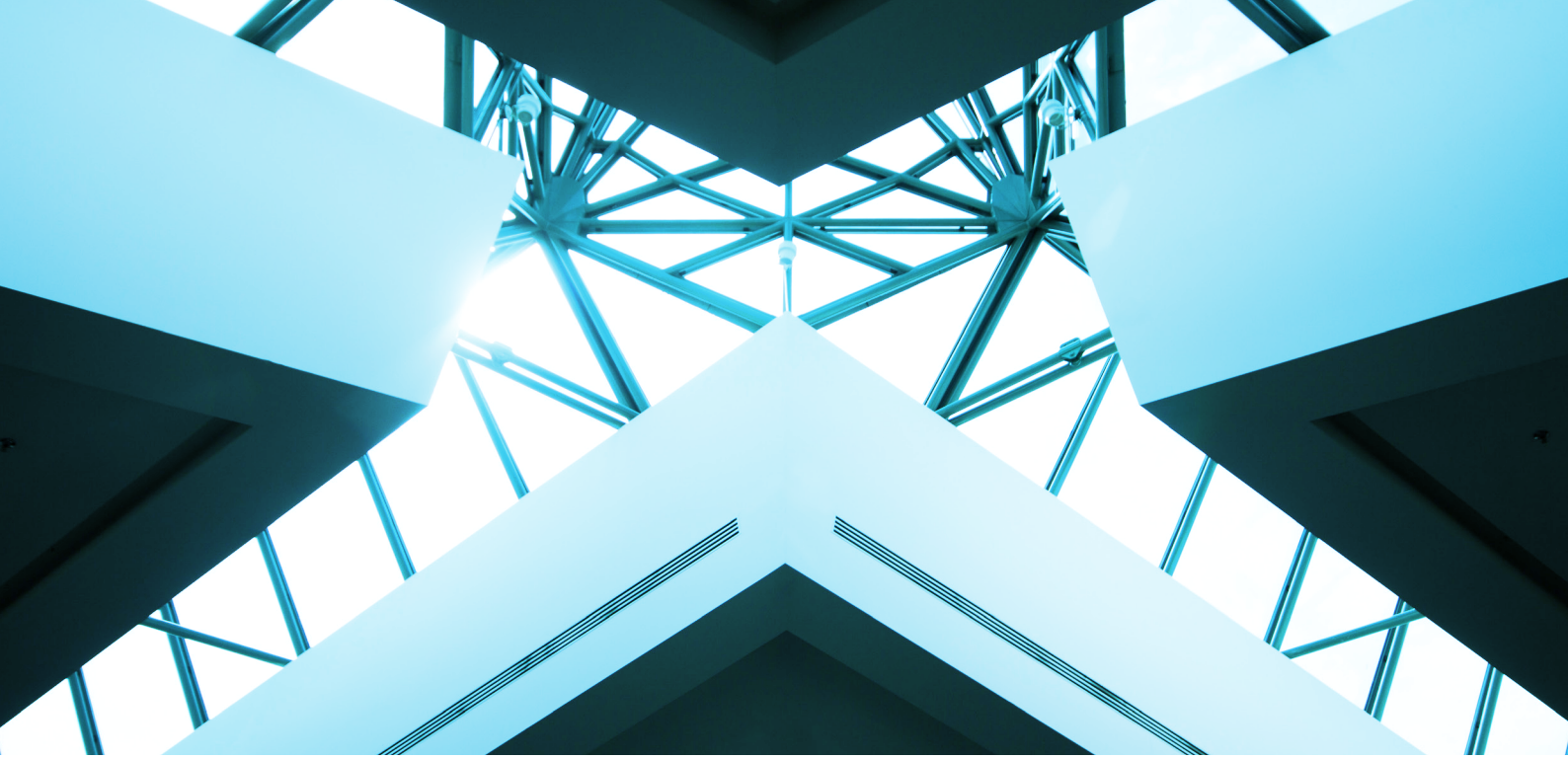
1. Establish a cloud security governance model

2. Update your cloud security policy and become compliant

3. Educate your staff

4. Optimize your logging and monitoring

5. Clarify roles and responsibilities between you and your service provider



Intro

It is easy to appreciate why the cloud has quickly become a backbone for most companies today. Cloud services offer superior flexibility, accessibility, and capacity compared to traditional online computing and storage methods.

Organizations have completed a lot of cloud transformation projects in recent years. Most companies have ended up in hybrid-models, where some assets and operations are stored in the cloud and others are kept on-premises. Hybrid models may be a realistic choice for some businesses, but the overall management becomes more demanding.

When the transformation is done, many CIOs and CISOs become concerned: *"Did we move to the cloud in a secure and smart way?"* That is a tricky question to answer – companies don't know what is happening in their cloud anymore. It's out of their hands, transferred to the cloud service provider.

The cloud seems easy to use and manage, but it keeps changing, new features come and go. The follow-up takes more time than in the old on-premises days.

Luckily, not everything needs to be learned by trial and error. We have gathered together the most common cloud security gaps and a to do list for you to rule your cloud.

Part 1: The most common cloud security gaps

Scalable and fast platform setups, IT cost savings, modern workplace tools, flexibility – the cloud benefits and supports modern digital business in many ways. Moving to the cloud is easy, as the cloud providers offer neat packages to outsource servers and data storage at a reasonable price.

What most companies haven't thought about is that **the cloud transformation impacts the organizational chart**. On-premises governance models don't work similarly in cloud environments, which are flexible, scalable, and fragmented.

Whether they have completed their cloud transformation or they are in the middle of it, we see organizations struggle in different areas.

> **"Sure, you can learn things by trial and error, but it's not the most professional way".**
>
> – Samu Nisula, Senior Security Consultant at Nixu

The lack of visibility

The cloud is managed by the provider, so there's no access to all the configurations, settings and data. That's why lack of visibility into infrastructure security is one of the biggest operational cloud security headaches IT organizations are struggling with.

When a mid-sized company has transferred their operations to a cloud service, an internal DevOps culture will usually form. They have small development teams, who independently build and test new environments in the cloud.

However, we have come across a key concern among companies: when their DevOps team is building different environments independently, they can't be sure that the cloud parameters are in order. Cloud configuration owners and policy makers need to allow internal teams the autonomy to manage their cloud services but they have no way to enforce any policies.

Usually, organizations are not aware of their security gaps until a cybersecurity audit has taken place.

No security policy or an old policy

It's difficult to be compliant when you don't see what is happening in your cloud. The need for a security policy is especially crucial in hybrid models.

Psst...! Struggling with how to keep your security policy and risk appetite on the right level? Let us help:

nixu.com/cloudtransformation

Even if a company has a cloud security policy, its guidelines and standards become outdated fast, thanks to the updates and modifications made by cloud providers.

What we typically see is that a company creates a cloud security policy and delivers it to the IT department for implementation. Then, maybe after a year or two, they run a security audit with alarming results. *"What on earth happened? Why haven't we been following our IT policy?"*, they ask. It's not that they didn't follow the policy. The policy just doesn't meet the requirements of the current threat landscape anymore and no longer addresses relevant business risks.

One of the main reasons for incidents and breaches in the cloud is misconfiguration. Way too often default settings fail to fulfill the desired security profile, or even changes done to it might have an effect other than what was expected. There is a great chance for configuration drift once you have comfortably settled in the cloud.

People make mistakes. We just need to identify and fix those mistakes before someone else exploits them. To solve this, one needs to constantly monitor the environment for changes and raise the alert or prevent the changes if they do not comply with policies.

Bad Identity and Access Management creates security gaps

During cloud transformation, extensive access rights are easily given to anyone to start up their projects and create their environments in the cloud. You quickly end up with multiple accounts and subscriptions and they all need their own security controls.

Easy access also creates security gaps. The usual cybersecurity risks also apply to the cloud environment: phishing, password spraying, brute force and DDoS attacks, as well as worms, are alive and kicking in the cloud environment. What makes the risk even bigger, is that once an outsider gets into the cloud network, it's easy to access all the company data. If a company has transferred its operational and critical assets to the cloud, the consequences accumulate.

Forgotten databases, third-party vendor risks, untimely de-activated accounts, inappropriate permissions and other identity and access management flaws are the key factors that have resulted in thousands of previous data breaches.

No time to keep up

When people work in the cloud without a wide perspective and knowledge, surprises are expected. You can easily open a server in the extranet or cause all kinds of configuration errors by accident.

The cloud environment keeps evolving: new features are added daily as the old ones are deleted. You can easily click your own favorite features on and off, and the whole thing seems intuitive. People are encouraged to be self-directed, but there's a lot to take in, even for a cybersecurity enthusiast.

Part 2: Your to do list to get control of your cloud

Cloud service providers are constantly expanding and developing their security services. The perception of the cloud is often that the vendors take care of security. That's not correct. The vendor secures their own systems and provides you with the tools needed to configure and activate security features on you own.

In the end, it's the customers' responsibility to secure their data in the cloud. Here's what you can do.

1. Establish a cloud security governance model

Many organizations feel lost after transition to the cloud, because the old on-premises governance model doesn't apply to the cloud. Effective and properly protected cloud use requires a proper governance model.

Establishing proper IAM policies that follow the principle of least privilege is of utmost importance. Who has access to your cloud environment? Which services do they want to use? Why do they need this access? These are just some of the questions one needs to answer when utilizing public cloud service providers.

Nixu have had cases in which customers have given subcontractors access to their cloud environments. Later, we have identified that even the employees of the subcontractor no longer work there, but their access to our customer environments has not been revoked.

Usually, you start building the governance model by defining your cloud service provider hierarchy and choosing your account model. Create a tree model of your organization in relation to your cloud environment. This is followed by defining and implementing technical controls, operational continuity, backup policies, etc.

As we tend to say, **cybersecurity loves good governance.** As in any environment, this also applies to the cloud.

2. Update your cloud security policy and become compliant

How well are you following the laws and guidelines on cloud data security concerning your business? Don't settle for an occasional security audit – **you can run security tests for your applications on your own schedule** defined in the security policy. Review your current state of compliance and adjust your service security level regularly.

Not in the cloud yet?
Start by creating a cloud transformation roadmap. Ask Nixuans about the roadmap!

nixu.com/cloudtransformation

Define the practical meaning of Declaration of Conformity for your organization.

Cloud services have started to offer compliance dashboards that provide new tools for measuring compliance. Regular internal (and external) audits are still needed, because so far, the compliance tools can't see everything, for instance the configuration of your own customized application.

3. Educate your staff

Cloud service providers offer a wide range of courses and educational material, but often organizations don't allocate enough time for self-studying. Service providers' education programs are free and of good quality. There are usually different training courses for different roles.

Psst...! Need help?
Nixu's cloud inspection will cover all these steps, including:

- Current state analysis & evaluation of findings
- Recommendations for enhancements
- Recommendations for next steps

Training takes time and is not a one-time thing. Define the type of training your organization needs and which key personnel should participate. Allocate working hours for training and monitor progress to make sure your staff has up-to-date knowledge. We can assure you that the time your organization spends on cloud education will pay off with fewer surprises and more peace of mind.

One way to measure your level of expertise is to list the cloud trainings and certifications your employees have passed. So, when you're asked, *"How have you handled your cloud security?"*, you can show your efforts supporting the education of your staff.

4. Optimize logging and monitoring

Who did what and when in the cloud? Do we have an incident? **Logging and monitoring optimization is crucial.** Not every feature is enabled by default, so you need to be active. Vulnerability management is similar in the cloud as on the premises, but the metrics vary.

Psst...! Are you interested in buying a cloud access security broker (CASB) but you're still hesitant about the right choice of technology? We have conducted a wide-scale evaluation on different CASB technologies and we are happy to share our findings with you. Let's talk more!

nixu.com/contact

If you're struggling with cloud monitoring, don't worry – you're like most companies. Create a cloud monitoring strategy. Start by figuring out the relevant log use cases in your business. Your cloud environment may have several integrations and you need to understand what log events you need to monitor.

It's important to understand the potential impacts on business when adding new features to existing cloud services. Create a threat model of the things that can go wrong and assess the risk level according to your business.

All threats won't likely be critical to your business and industry, but you should have a clear priority list of what to protect first.

5. Clarify roles and responsibilities between you and your cloud service provider

We often see too permissive access rights in cloud environments. One bad example was an organization that transferred all its access rights from on-premises to the cloud without checking them. It turned out that they had 400 end users and 110 admin users. That was a surprise.

Create a matrix where you can clearly see responsibilities. You can use a responsible, accountable, consulted, and informed (RACI) matrix, your current organizational chart or anything that works for you. Remember that even though you have outsourced your data storage to a cloud service, you still have responsibilities, and an assurance policy needs to be in place.

Migrating environments and services to the cloud provides several benefits but this transformation also includes risks that should be handled accordingly. We ensure that your cloud environment is set up in the correct way, no matter whether it is utilizing IaaS or PaaS when building your own applications, migrating current systems to the cloud or utilizing SaaS in individual functions. With the help of our cloud security specialists you can rest assured that the cloud you have built or deployed is secure and the associated risks remain at an acceptable level.

Contact us so we can make sure together that your migration to the cloud is conducted in a proper way.

Sources:

CheckPoint: 2019 Cloud Security Report
https://pages.checkpoint.com/cloud-security-report-2019.html

UpGuard: The RNC Files: Inside the Largest US Voter Data Leak
https://www.upguard.com/breaches/the-rnc-files

Azure enterprise scaffold is now the Microsoft Cloud Adoption Framework for Azure
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/reference/azure-scaffold

Centrify: Reduce the Likelihood of an Attack Through anIAM Maturity Model
https://www.centrify.com/lpforrester-stop-the-breach-IAM-maturity-model/

IBM: Clarify roles and responsibilities by using a RACI matrix
https://www.ibm.com/garage/method/practices/manage/raci-matrix

nixu cybersecurity.

Contact:

/nixuoy
@nixutigerteam
/company/nixu-oy/
nixu.sales@nixu.com
www.nixu.com

Nixu is a cybersecurity services company on a mission to keep the digital society running. Our passion is helping organizations embrace digitalization securely. Partnering with our clients, we provide practical solutions for ensuring business continuity, easy access to digital services and data protection. We aim to provide the best workplace for our team of over 400 cybersecurity professionals with a hands-on attitude. With Nordic roots, Nixu serves enterprise clients worldwide. Nixu's shares are listed on Nasdaq Helsinki's official list.