Microsoft Azure Security Assessment

On the way to a secure future in the cloud

Have you opted for the cloud? If so, then don't underestimate the transformation to a secure cloud environment. Not only do you need to transform all your solutions. You also need to take care of the digital tools that your clients use and enhance your knowledge of a properly secured cloud environment. The ideal first step? A Microsoft Azure Security Assessment.

The challenges of the cloud

Moving your applications to the cloud and the transition to a secure cloud environment brings with it many benefits for your organization: **improved business processes, more efficient working**, and a **better service** for your clients and IT partners. You also make your business more flexible.

To get the max from the cloud, your employees must be able to access your data and applications in the cloud on every device and via every network. That comes with new risks and requires **new cybersecurity measures**.

You will need to:
- Secure your cloud environment with access control.
- Clearly define everyone's tasks and responsibilities.
- Protect sensitive client and business data from data leaks.
- Replace your traditional security solutions with cloud security.

At the same time, at the Management's request, you need to keep **costs under control** and conform to the **legal requirements** when migrating data to the cloud. You can meet all these requirements by implementing the right security strategy and measures.

proximus
enterprise

100% secure cloud architecture

The Proximus Azure Security Assessment will provide you with a **realistic picture** of:

- The **cybersecurity risks** that your company is exposed to **right now**.
- The **threats** that you will be facing in the **future**.
- The **options** available to you for **securing your cloud environment**.

We will give you the **best practices in cybersecurity** and you will find out how to tackle security challenges as efficiently as possible:

- We smooth the way to an efficient **cloud-centered strategy**.
- You learn how to **build an IT architecture** that secures your cloud environment.
- We make sure that the **securing of your Azure environment** is carried out according to those best practices and the needs of your business.

Your Azure Security Assessment in 5 steps

A **standard Azure Security Assessment** takes about **1 month**. You can supplement the assessment with **extra workshops or managed services that we tailor to your company's needs**.

The assessment consists in:

1.
A pre-engagement meeting

2.
The technical set-up
- Kick-off workshop
- Azure Workshop
- Technical set-up

3.
Collecting all data (3 weeks)

4.
The joint identification of threats

5.
The presentation of the results and your security plan

The entire evaluation **minimizes the workload** on your IT teams as much as possible and has absolutely no impact on your end-users.

In your own Microsoft environment

We only use Microsoft tools to analyze your security logs and warnings. And **we process all information in your own Microsoft tenant**. This means that your data remains secure in your own environment.

Including evaluation of real security breaches

In your evaluation report, we not only evaluate your cybersecurity policy and measures but we also include a number of security issues that occurred at your company during the period in which we collect your data.

After the assessment

We are also there to help after the assessment, if required, for the configuration and management of your cybersecurity.

Why Proximus?

- More than 15 years' experience in cybersecurity.
- Experience in all sectors: services, industry, finance, government, …
- Our Microsoft Gold Partner for Security award means that you are guaranteed the best service and the best advice at all times.

Find out more?

Contact our expert via proximus.be/securitycontact

proximus enterprise