nviso

www.nviso.eu

Cloud Secure Design

Service Presentation & Proposal

About NVISO

Get to know us better

Our Company

NVISO is a pure play **Cyber Security consulting firm** since 2013 with 90+ specialized security experts.

Initially founded in **Belgium**, we opened offices in **Germany** (Frankfurt & Munich) in 2018!

Our mission is to **safeguard the foundations of European society from cyber attacks**.

Our DNA

Pride: We are proud of who we are and what we do.

We care: We care about our customers and people.

Break barriers: We challenge the status quo by continuous innovation.

No BS: We keep our promises and don't fool around.

Our Research

We invest 10% of our annual revenue in research of new security techniques and the development of new solutions.

Follow us on :

@NVISOsecurity and @NVISO_Labs

blog.nviso.eu/

Our Services

We have a **strong track record** providing information and cyber security services to the **Financial Services, Government & Defense** and **Technology** sector.

NVISO can support you throughout the **entire cyber security incident lifecycle**.

Cloud Security Services

An overview of our cloud services

Microsoft Azure

Microsoft 365

In case you are thinking about **moving towards the cloud** or you are **already in the cloud** NVISO can assist you in both cases. Our cloud security services can range from an integrated security design in your new environment to reviewing your current infrastructure via our standardized security assessment.

Cloud security assessments

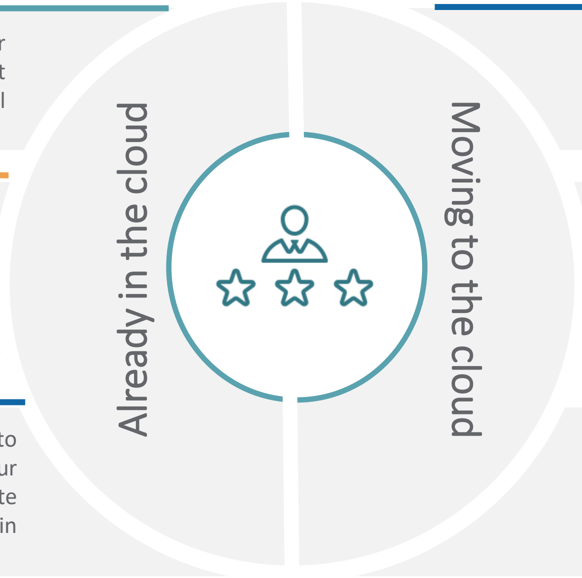
How secure your current environment is? Our assessment provides you an overview about your current exposure, missing security controls or typical misconfigurations within cloud environments.

Cloud ASTRO Managed Service

As your cloud environment is changing, you will need to continuously monitor your current configuration state. and adapt your security requirements continuously. Within our ASTRO managed service, we will provide a baseline, compliance monitoring and improvements.

Cloud security compliance

As new cloud resources are deployed, you will need to ensure that **compliance** of each cloud resource to your **corporate security standard**. NVISO can help you create automated compliance checks and reporting to gain visibility and additional compliance rules.



Cloud secure design

NVISO can assist **you within the design process to integrate security in your design** based on your requirements, industry best practices and our technology expertise.

Cloud security Engineering

Continuously integrate our security expertise in your cloud environment. During the design phase we will **define and review the security controls**, in a later stage our security architects review **ongoing changes and support your operational teams.**

Cloud security roadmap

Define the security roadmap for the cloud services used withing your organization through workshops and setup cloud infrastructure for your organization defining **quick wins and structural recommendations**.

Secure Design

Our approach

Overview of our project method

KICK-OFF

In the kick-off meeting, the project conditions are defined. All agreements are documented and provided to all project participants.

WORKSHOPS

This phase focuses on conducting the workshop activities. At the end of the workshops, we will conduct a gap assessment and agree upon the further procedure. Regardless of the project phase, identified critical misconfigurations or design issues will immediately be communicated to the customer.

REFERENCE MODEL

The secure design exercise results are documented in a detailed design document. In addition, we will conduct a joint debriefing session to present our approach to this refence model to the responsible persons and to discuss open questions.

Follow UP

Further assistance might be required, this can include policy development or cloud engineering, these services are typically provided in T&M mode and are optional.

Kick-Off Meeting

Contents

PROJECT CONDITIONS

Agreeing on key milestones

Selecting a single point of contact who can be reached in case of an emergency and towards whom we can raise critical vulnerabilities during testing

Gathering requirements and expectations

Scheduling, plan the workshops

Determining the target design / objectives(remote or on-site)

DESIGN ANALYSIS

Understanding the **business impact, how your organization works in the cloud** and discussion of **threats** connected to the use of cloud.

Identifying what is key to protect and how the cloud environment is being used from a business perspective. **Identification of critical assets such as data or certain services**(„Crown Jewels“)

Create an inventory of available documentation related to cloud design, governance and typical procedures/ processes to follow

DESIGN DETAILS

Creating **Abuse Cases** based on the key features, assets and risks the environment faces

Defining desired refence model based on:

- Type of cloud services and deployment models
- Type of assets and information hosted in cloud environments Access to source code
- Organizational mapping on cloud environments.
- Best practices based on the technology stack in place

Secure Design Workshops

Goals and Objectives

Understanding of the following design principles

Cloud Governance

The objective of this phase is:

- gaining a detailed understanding of the structure within you cloud environment
- the logical segmentation based on subscriptions or accounts
- network Model & Topology in place

During the workshops its key to understand how logical dependencies are defined between departments, management groups, resource groups, 3rd party access and overal security and compliance teams.

Mapping the different roles and responsibilities (department level) is essential to create a cloud reference model that will work for your organization.

Access Management

The information obtained during the workshops will also have a key focus on how identity and access management is enforced, typically we look at common factors such as a single authentication service, strong authentication, IAM policies and priviliged access roles.

In our reference model it‘s important to understand how actors are using your cloud environment, typically the following actors are considered:

Internal	External
Regular user	Internet user
Developer	External consultants
Engineers	3rd party providers
Administrators	

Data & Applications

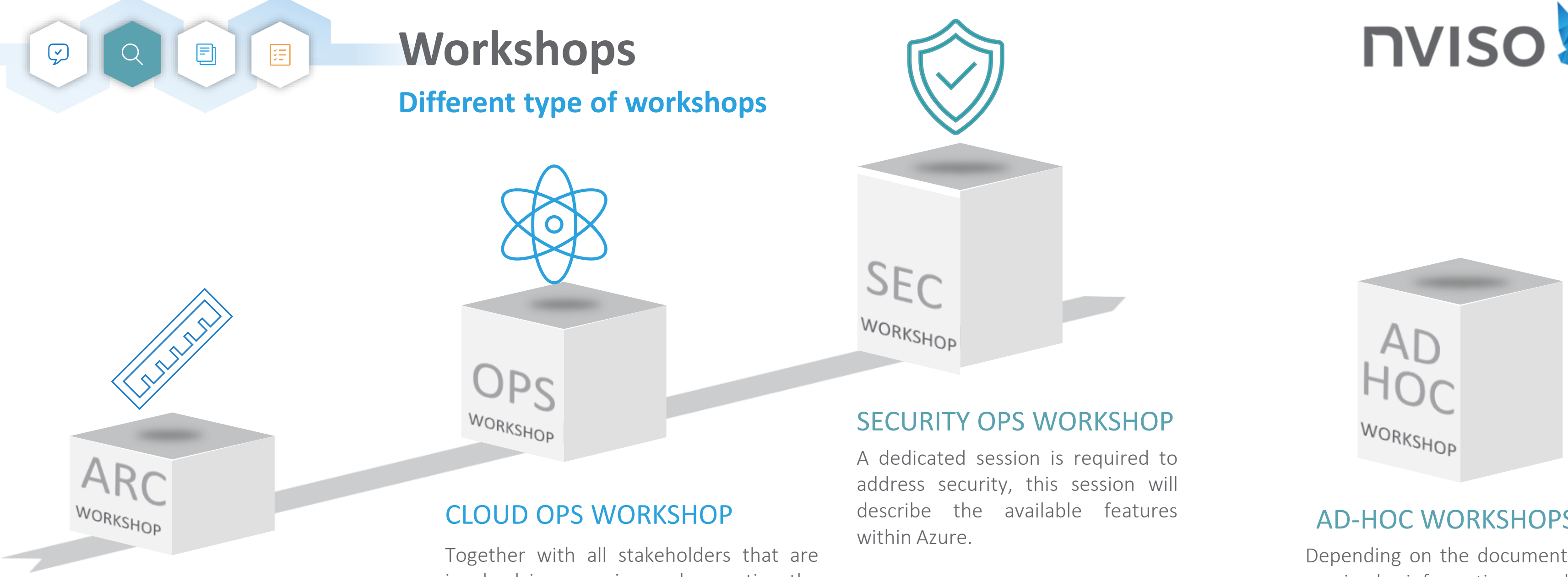
A reference model takes into accounts the assets needed to protect, our reference model is linked to the type of information being saved or processed and the criticality of the assists and service in your cloud environment.

The resulting Proof-Of-Concepts (POC) are part of the assessment report. They help customers reproduce certain vulnerabilities. Depending on the criticality a policy will be described based on the following categories:

Secure configuration	Security Monitoring
Access control	Application control
Networking	Data protection
Infrastructure provisioning	Compliance monitoring

Workshops

Different type of workshops



ARCHITECTURE WORKSHOP

Coordination with your enterprise architects NVISO will review the current specifications on enterprise architecture and implemented security controls.

These controls will be translated toward security controls available in the cloud

CLOUD OPS WORKSHOP

Together with all stakeholders that are involved in managing and operating the cloud environment.

The current operational model is reviewed and based on the documentation, processes and controls in place we will define the most optimal path and controls required for your environment.

SECURITY OPS WORKSHOP

A dedicated session is required to address security, this session will describe the available features within Azure.

Based on your input several architectural decisions and selected security controls integrated into the design.

We also need a clear understanding about the visibility required from a security perspective.

AD-HOC WORKSHOPS

Depending on the documentation , received information and less mature environments additional workshops can be required .

In case required additional workshops can be scheduled but is limited to 2 within the current estimation.

Building your refence model

Develop Refence model

Supporting security activities

Bussiness Objectives

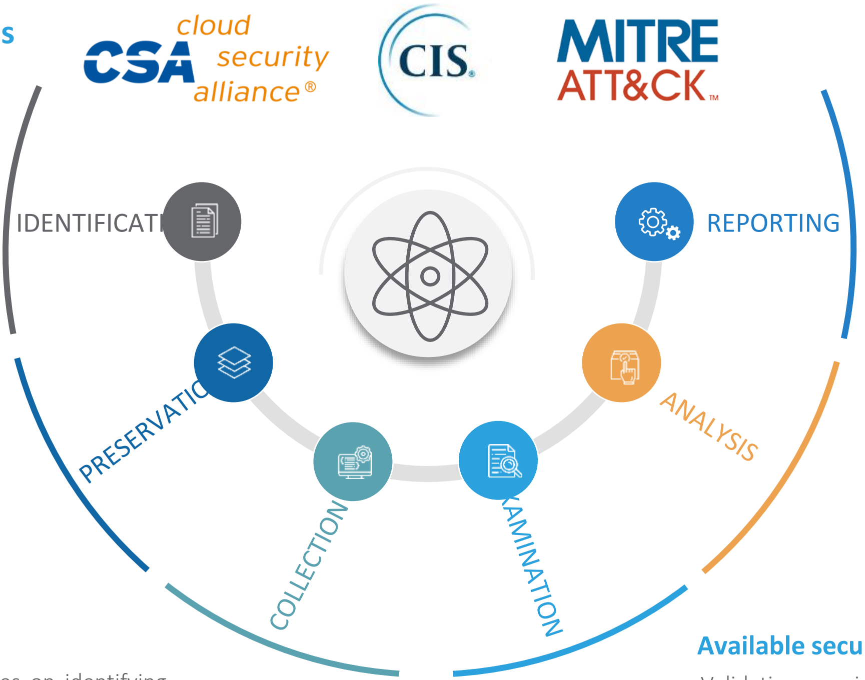
Threat modelling identifies threats and mitigations affecting an application and thus serves as a basis for creating a secure design.

Technology Design

Reviewing the current security controls in the application architecture helps identifying potential security flaws at an early stage.

GAP Assessment

A code analysis focuses on identifying security weaknesses and vulnerabilities introduced in the application's source code.



Document Reference Model

Frequent assessment to re-evaluate the security posture of the application and to ensure that a good level of security is maintained over time.

Define standard policy

Offering rewards to those who identify errors and vulnerabilities in an application boosts security by leveraging the knowledge and skills of the entire security community.

Available security Controls

Validations aims at verifying the application's compliance with security baselines and identifying critical security weaknesses.

Controls Covered

Security categories in our reference model

Cloud governance

Network Model

PaaS, SaaS and IaaS

Secure configuration

Compliance policies

Exposed services

Data protection

Traffic filtering

Logging & Monitoring

Identity & access

External actors

CSA cloud security alliance®

Azure & M365 Security Product Portfolio

A selection of cloud-native security features

NVISO has expertise with several cloud-native security controls available in Microsoft 365 and Azure; this list a selection of the most common features that organizations are using.

- Azure AD
- Azure PIM
- Security Groups
- Security Center
- Azure Defender
- Azure Sentinel
- Intune
- Azure Monitor
- Azure Policy
- Defender for Endpoint
- Information Protection
- Cloud App Security (MCAS)
- Conditional Access
- Own analysis tools

Depending on your licenses, additional costs and requirements more advanced security controls are described in your reference model.

Looking for specific expertise, we have a team of dedicated cloud engineers that can support your team, **get in touch for a customized proposal !**

Reporting and Project Closure

Reporting

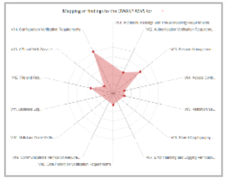
In the course of the assessment, the customer receives regular status meeting updates the project progress and vulnerabilities already identified. Therefore, no new vulnerabilities should be identified in the reporting phase.

The report will be provided in PDF format.

nviso

Azure target design

Configuration and as-built documentation for our centralized Azure environment



Design Decision: *Client will follow the service line-based pattern to allow flexibility within these environments toward the service lines. The following service lines were defined during the design phase: shared services, prd, non-prd and UAP and development*

Executive summary:

- detailed description of the identified gaps and recommendations
- Mapping to CIS benchmarks and prioritization of structural improvements.

Overview of:

- Scope
- Objectives
- Procedure
- Target Design

Detailed design overview with design decisions described during the workshops:

- Azure Governance and Architecture
- Identity and Access Management model
- Network security model
- Secure configuration model
- Platform management and monitoring
- Optional: DevSecOps – infra as code

Appendix with further information on technical aspects or gaps:

- Documentation to the solution
- Evidence of misconfigurations

Project Closure

After reporting, the results can be presented to different audiences:

A **technical workshop** with your teams to ensure that the security controls are correctly implemented and configured according to our target design. This can be done via follow up sessions with your technology experts

A final **presentation to the management** will explain:

- the design and analysis performed
- Structural improvement points– explained at a non-technical level
- measures to improve the overall cloud security levels

The **feedback session** with the customer aims to get feedback on the assessment execution and customer communication. This enables NVISO to continuously optimize its services and to further expand and improve the cooperation with the customer in the future.

delaware

NVISO has forged a **unique partnership** with technology expert and Microsoft Gold partner delaware. This partnership can assist you with **the full migration and implementation towards Azure**. NVISO experts will remain their focus the security requirements and delaware experts will implement the technology stack according to the target design.

Our People & Financial Proposition

World-class service at a fair price

Our People

We will assemble a team of experts to conduct this engagement.

QA Pool

Quality Assurance is performed at various stages of the project (planning, execution, reporting…) by experienced security professionals. These experts are drawn from our Expert pool.

Expert Pool

NVISO has a team of **highly skilled expert professionals** available that will serve as an Expert to assist in your cloud security projects. This pool exists of people having **+5 years of experience in cloud security and architecture**, some examples are included in the CV section.

Service Delivery Manager

Jeroen Vandeleur, service line lead at NVISO with 15 years of experience in cyber security architecture. He is leading NVISO's cloud security service line.

Escalation level
Account management

Project Manager

Stijn Wellens is a Project Manager at NVISO with 5 years of experience in cloud security. He developed cloud security roadmaps fo AWS and Azure. Stijn is technical solution lead for Cloud Security services at NVISO.

Coordination
Planning
Management

Consultant Pool

Execution is performed by professionals from our Belgian and/or German consultant pool.

Execution

Our References

An overview of our recent engagements

nviso

Some of our references

We have done this before – Cloud Security

Cloud Security Architect	Industry: Utilities Workload / Cost : **20 MD/ Year** Country: **Global**	NVISO has been elected as a service provider for all cloud security architecture on Azure and Office 365 for a global company that provides services to the utilities sector. This engagement include architecture reviews of the current setup, define and propose a blueprint that is NIST compliant and assisting future projects with the configuration and optimization of security features within Azure and O365.
Cloud Security Incident	Industry: **Financial services** Workload / Cost : **5 MD** Country: **Belgium**	Within NVISO we have a managed detect and respond team and several contracts with our clients to detect and respond on security incidents. NVISO involves cloud security experts in case a cloud security incident was detected. During the incident NVISO was able to provide insight into the O365 account compromise and the data that was exfiltrated during the attack. Based on the incident we provided actionable recommendation to improve the detect and respond capabilities within that organization.
Hybrid Monitoring model	Industry: **Pharmacy** Workload / Cost : **17MD** Country: **Belgium**	NVISO developed a SOC target operations model including a hybrid setup. The objective was to benefit from the cloud security toolset and integrate this with a centralized monitoring solution. Within this model we were able define the governance structure and processes within that organization. Technical use case implementation was done based on the MITTRE ATT&CK Framework.
Cloud Security Assessment	Industry: **Financial services** Workload / Cost : **7 MD** Country: **Belgium**	NVISO was requested to review an API based banking platform developed in the cloud, this projects was part of the PSD2 guidelines published by the European Central Bank. The application was hosted in AWS and we executed several compliancy checks against the CIS benchmarks to identify potential gaps and additionally a penetration test was performed on this environment.

For confidentiality reasons, we may not disclose our customers' names: upon request, however, we are happy to request our customers to be contacted by your team for reference.

We know cloud security

And actively stay on top of our game

Cloud environments are becoming increasingly complex, and complexity can introduce severe flaws with real consequences if they are not mitigated in time. Over the years, NVISO has built the right toolset and expertise to tackle a broad range of cloud features and cloud related technologies.

We break barriers – We research new technologies and share our findings with the community.

See Azure Automation , Detect ZeroLogon , Azure security logging

We build the tools – We created a PowerShell and python scripts to assess several cloud functionalities and collect evidence to look at misconfigured settings.

We help define the standards – We are recognized and contribute to the Microsoft Intelligent Security Association.

We share our expertise – Within the cyber security coalition we organized the cloud experience sharing day.

We are certified – Our team has several certificates such as GDAPT, AZ-500, MS-500 CSSP (Certified Cloud Security Professional).

NVISO also develops courseware related to SANS 401 which includes an introduction towards cloud security.

Appendix

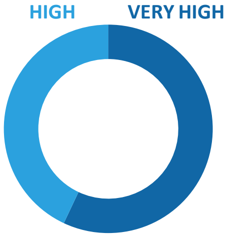
Our Quality Delivery

Top quality

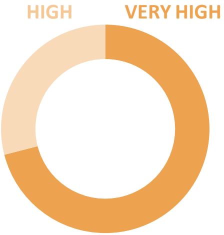
What our clients tell us

We take pride in our positive feedback.

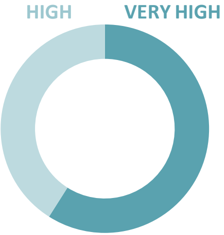
Upon completion of each engagement, we perform an engagement performance assessment together with our clients.
The following charts represent our clients' responses for NVISO engagements performed over the last 12 months, on scale from Low to Very High.



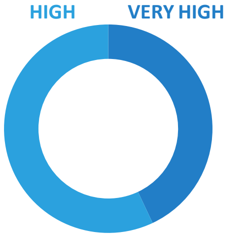
How satisfied are you overall with the engagement?



How do you rate NVISO's responsiveness to your questions or concerns?



How do you rate NVISO's expertise related to the issue at hand?



How do you rate the quality of deliverables and services rendered?

> Since February 2013, NVISO is one of our preferred suppliers for information security assessments. During these 2 years, they have been involved in a wide variety of assessments, going from infrastructure-level assessments on hosts and entire solution architectures to performing code reviews on some of our critical applications. We believe the fieldwork and deliverables supplied by NVISO are of very good quality, thereby finding a good balance between providing sufficient technical detail, but also describing issues in a language understandable to the business. Furthermore, we very much appreciate NVISO's flexibility and responsiveness to our needs.

BNP PARIBAS

Azat Nabiullin
Manager Technical Security Services

”

We first asked NVISO to deliver a secure development training to our development community in Q3 2014. The training, which was developed and delivered by NVISO's software security experts, was very well received by our developers. The main reasons they cited were the good balance between sufficient theoretical background and practical exercises. In follow-up engagements, NVISO is performing a forensic readiness assessment for us, and has also assessed our Windows Phone banking platform. We are very much impressed with NVISO's technical expertise and customer focus. They do not hesitate to go the extra mile to ensure your expectations as a client are met (or even exceeded).

Belfius

Karine Goris

Head of IT Security, IT Risk and DRP

> NVISO has been very responsive to our needs and has exceeded our expectations by bringing a very high standard of skills and dedication into their work

bpost bank

Wouter Van den Kerkhove
Chief Risk Officer

”

Very competent, friendly and accessible during training courses. Furthermore, NVISO produces the most relevant web applications pen-test reports I have seen so far

BUY WAY PERSONAL FINANCE

Yvan Torres Fally
Software Architect

NVISO has helped us on a number of information security related projects since 2013. This ranges from providing secure architecture advise to performing security assessments on our online banking platform. We were charmed by NVISO's no-nonsense approach that is a perfect match for Argenta's own house style. NVISO's professionals consistently demonstrate a high level of technical expertise and professionalism. Furthermore, I'm very pleased with NVISO's persistent customer focus and quality delivery.

ARGENTA
uw appeltje voor de dorst

Patrick Augustijnen
ICT Service Governance Manager

HACKED ?

CALL (24 h)

+49 89 38 03 59 57

NVISO • Security. Research. Risk.

www.nviso.eu