



Cloud Compliance and Security Inspector

A PwC Product

**Security and compliance for
multi-cloud environments**

Content

1.	Your challenge	03
2.	Our solution: Cloud Compliance and Security Inspector	04
3.	Special features	06
4.	Use cases	07
5.	FAQ	09
6.	Contact	10

Your challenge

Hundreds of configurations affect the security situation of cloud environments. Even a single misconfiguration can lead to major consequences for companies.

The verification of misconfigurations is often very complex. Moreover, the results are not comparable, as all cloud providers use their own assessment methods.

To meet compliance requirements, automated and regular verification of the effectiveness of cloud controls is necessary.

62%

of all publicly reported security incidents in cloud environments were due to misconfiguration¹

Preventing misconfigurations is priority number


1

in Cloud Security²



¹ Fortinet | 2022 Cloud Security Report

² ISC2 (ISC2 Foundation); Cybersecurity Insiders | 2022



Our solution: Cloud Compliance and Security Inspector

PwC's Cloud Compliance and Security Inspector is a platform-based application for assessing and monitoring security configurations in hybrid-cloud and multi-cloud environments (AWS, Microsoft Azure, GCP, etc.).

Our tool offers:

- **Standardisation:** A scoring system developed by PwC provides comparable assessment results on the security of multi-cloud environments.
- **Benchmarking:** The solution verifies the compliance with various standards and leading practices, e.g. NIST, CIS, ISO, independent PwC good practices or self-generated good practices.
- **Compliance monitoring:** The tool enables continuous monitoring of compliance with standards or user and authorisation audits.

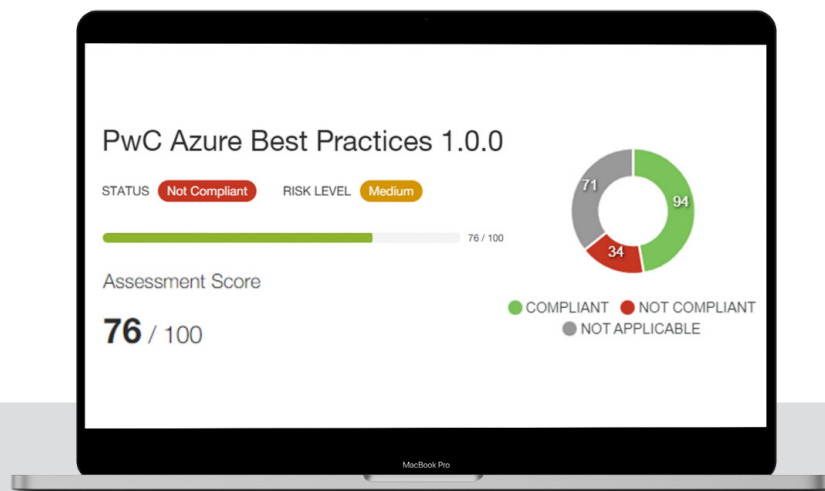
Your benefits at a glance:

- Get an independent and holistic understanding and overview of cloud security processes
- Reduce costs and time for audits
- Comply with relevant safety standards such as ISO, NIST and CIS
- Identify potential security vulnerabilities in cloud configurations
- Get a total package of technical transparency paired with knowledge expertise-based holistic advice

Our solution: Cloud Compliance and Security Inspector

Core functionalities of the Cloud Compliance and Security Inspector

Assessments are carried out using the tool to evaluate and monitor security configurations in multi-cloud environments. Here, a cloud account connected to the tool is checked with regard to a selected benchmark and the requirements contained within it.



More core functionalities at a glance

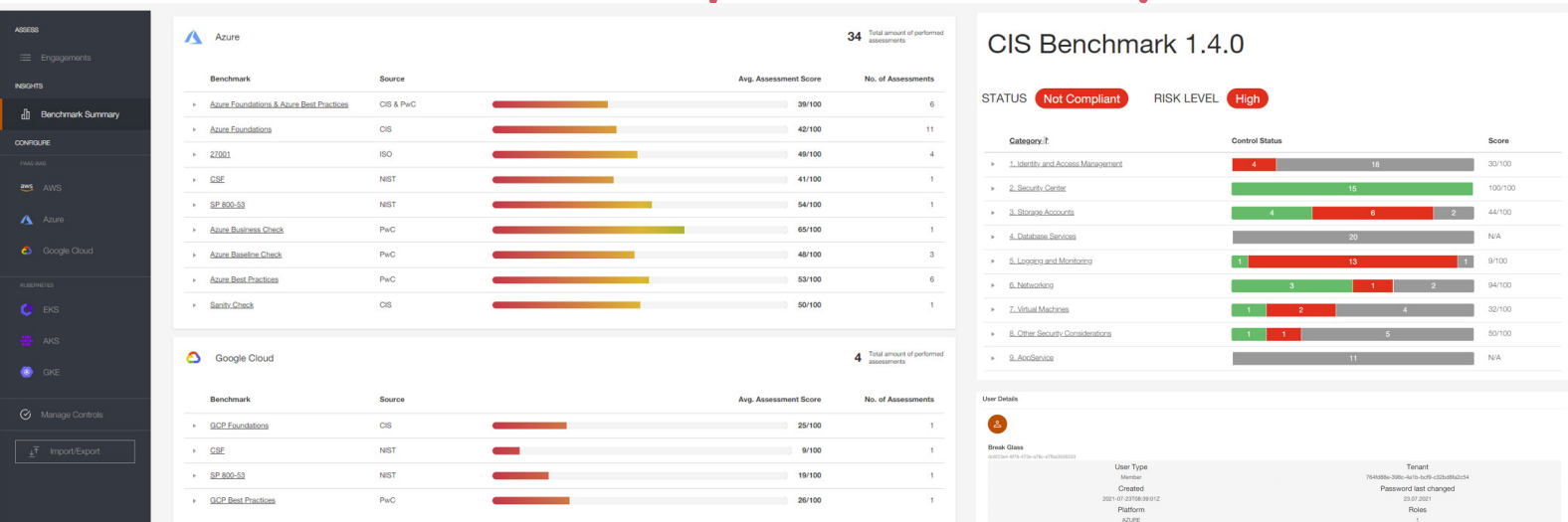
- Connects to the most popular cloud environments from different cloud providers such as Microsoft Azure, Amazon AWS, Google Cloud Platform, Microsoft Office 365, etc.
- Enables automated monitoring of a multi-cloud environment and progress monitoring of security status.
- Provides hundreds of integrated and automated security controls as well as a view of the controls of different domains, e.g. Identity and Access Management (IAM), data and infrastructure security.

Special features

In addition to the core functionalities, the Cloud Compliance and Security Inspector offers several features for a better overview of the security situation of the cloud environment.

The **benchmark summary** provides an overview of all assessments that have been carried out. Using the **NIST, CISO, ISO** and **PwC Good Practices** standards, the security situation of the individual cloud environments can be compared with each other.

The **dashboard function** offers several progress monitoring features as well as the display of the security status of the security domains included in the benchmark.



Benchmarks are available for the most widely used IaaS and PaaS providers: **AWS, Azure** and **GCP**. Furthermore, dedicated checks are offered for the Kubernetes services of the providers (**EKS, AKS** and **GKE**).

By checking user and privileged accounts, the **IAM module** supports the continuous monitoring of compliance with user and authorisation audits.

Use case:

Optimising the security of the Azure environment

Internationally active food retailer

Initial situation

- As part of a cloud transformation project, missing or incorrectly configured security controls must be identified for the Azure environments.
- For this, the tool scanned the Azure environments of the customer.

Result

- Through scans, a large number of missing or misconfigured security controls have been detected, analysed, documented and fixed.
- The repeated scanning of the environments has made progress visible to the customer.
- The security of the Azure environments could therefore already be increased during the cloud transformation project. As a result, security measures are implemented at an early stage on a procedural and technical level.



Use case:

Assessing the security of a multi-cloud environment

International direct seller of frozen food and ice cream

Initial situation

- The client already operates a multi-cloud environment using both Microsoft Azure and Google's Cloud Platform. He wants to assess the security of his environments to identify faulty security configurations or security measures that have not been implemented or have only been partially implemented.
- To achieve this, the environments have been scanned with the tool.

Result

- The scans revealed that a large number of cloud processes and security configurations are not correctly established and implemented.
- Recommendations for action to mitigate critical security risks were identified at both the process and technical level.
- The next steps and the time horizon for mitigating the risks were visualised in a comprehensible way for the customer by means of a security roadmap.



Answers to the most frequently asked questions

How does the connection of the tool work?

For the connection, only a few configuration steps need to be carried out on the customer side, such as setting up the necessary authorisations. Instructions for the connection are available for the cloud platforms to be connected.

What impact will the scan have on my cloud environment?

The Cloud Compliance and Security Inspector only receives read access to the cloud environment. Performance losses or deterioration of the user experience are excluded.

How can clients use the tool?

Customers can choose between four models:

- **Baseline check:** quick assessment of 5 cloud security domains
- **Full-scope assessment:** a fully comprehensive cloud assessment with detailed risk analysis and management report
- **Managed Service:** assessments as a Managed Service by PwC with regular benchmarking and reporting
- **Software-as-a-Service solution in a licence model:** access to the tool for own assessments

More information on the models can be found at:

<https://store.pwc.de/en/products/cloud-compliance-and-security-inspector>

What happens with the data in the Cloud Compliance and Security Inspector?

At the application level, only the login data (e.g. user ID) is processed in the tool. Data processing is carried out on databases which, like the tool itself, are hosted in the German PwC infrastructure. These instances can only be accessed via the tool itself. Personal data is not transferred to different countries.

Can the controls be flexibly adapted to the clients' needs?

The integrated benchmark can be edited individually. In addition, the import function offers possibilities to adapt the controls to be audited to one's own company needs.

In which way can customers create their own benchmarks?

Customers can flexibly develop their own control catalogue for the creation of their own benchmarks. They can combine different standards such as ISO and CIS for their own benchmarks.



Visit our PwC Store! Here you will find all current prices for the Cloud Compliance and Security Inspector.

Ensure security and compliance for your multi-cloud environments. We tell you how.



Aleksei Resetko | Partner | PwC Cyber Security
aleksei.resetko@pwc.com



Vladyslav Dunajevski | Senior Manager | PwC Cyber Security
vladyslav.d.dunajevski@pwc.com



Patrick Nahm | Manager | PwC Cyber Security
patrick.nahm@pwc.com

