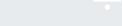# The first SOC 1 & 2 compliant Dutch Managed Service Provider on Azure

CHALLENGE

To improve the already high standards of security and compliance even more in both private and public cloud environments, Solvinity included Microsoft Azure in its annual SOC audit scope.

SOLUTION

With additional training on public cloud and obtaining relevant Microsoft certifications, the Security & Compliance team has succeeded in mapping the best practices of the Solvinity private cloud to a public cloud environment.

Meet the strict SOC 1 and 2 requirements when data is in the cloud

The strict SOC 1 and 2 standards are crucial for the confidence of organisations with high compliance requirements, such as banks, insurers and government, to be able to demonstrate that their data is in good hands. When their data is not on premises and they use the public cloud, this presents additional challenges. A managed IT service provider with SOC 1 and 2 in the public cloud unburdens and offers extra assurance and control.

A compliant infrastructure

The digital world is being increasingly regulated to protect sensitive personal information and prevent abuse. Some organisations only have to comply with general privacy legislation like the GDPR. Others are under more stringent supervision from government watchdogs. To satisfy the requirements of these institutions, organizations have to prove their client data is in good hands - even when their IT is outsourced.

> *This unique service in the Netherlands fits well with our experience of Solvinity: a thorough partner with an eye for innovative solutions.*

Harry Tolsma, Technology Strategist Microsoft The Netherlands

RESULTS

Solvinity became the first Dutch Managed Service Provider (MSP) with SOC for Azure, receiving glowing SOC 1 and 2 reports which led to increased trust from Solvinity clients.

Having an MSP deliver the SOC reports on Azure on top of Microsoft's compliance reports ensures organisations that the management of their Azure environments is in very good hands and is managed in a secure and compliant manner.

ABOUT SOLVINITY

Solvinity provides Secure Managed IT Services for organisations with high security requirements. With innovative cloud solutions, outsourcing, managed hosting and Lango Workspace, Solvinity supports the government, municipalities and leading organisations in financial and business services in their digital transformation. In addition, the company provides CI/CD, container technology and "Stretched" DevSecOps solutions for software developers. The organisation has distinguished itself with very high standards for cyber security and certifications according to (inter) national standards such as ISO 27001, ISO 14001, ISO 9001, SOC 1 & SOC 2 (including Azure) and PCI DSS. In 2020, Solvinity achieved an annual turnover of 50 million euros with 300 employees.

÷ **Solvinity**®

Secure Managed IT Services

Getting SOC 1 and 2 for Azure

"At Solvinity, we have been SOC compliant for our Solvinity private cloud for close to a decade," said Paul Cattermole, senior compliance officer at Solvinity. He continues: "But now that many organisations are discovering the scale benefits of the public cloud, we knew we had to expand our scope in terms of security and compliance." Azure was a logical step in the public cloud, not least because of the Gold partnership with Microsoft on the Azure Cloud Platform and as a Cloud Productivity Partner. This was quite a big challenge, because whilst public cloud wasn't new to Solvinity, it was new from a compliance perspective. Solvinity's public cloud team and Microsoft's certification programs provided the knowledge and expertise to achieve this result.

The Security & Compliance team has made a conscious decision not to write specific controls for Azure environments, but to map its existing ways of working into the techniques of the public cloud. This approach allows Solvinity to design its processes to a point where, whether working with a private or public cloud, it's confident they are in control.

A good example is access control for joiners and leavers. This is the basis which is used for controlling who has access to which customer systems. This process is synced from the HR system into the Active Directory and then into the Azure Active Directory (AAD). "Our role based access control checks were extended, to include AAD groups for customer systems. So while we have extended into the public cloud, our general compliance controls stay the same", Cattermole explains.

> *With Azure and Solvinity, FRISS is supported in its global expansion to deliver a safe, secure, scalable solution to fight fraud and high risks for property and casualty insurers.*

Christian van Leeuwen, Co-founder & CTO at FRISS

SOC reports to be proud of

In a hybrid world, it shouldn't matter what system you work in. It comes down to one simple fact: an independent auditor needs to be able to make a judgment about whether you have your affairs in order. Public cloud increasingly offers advantages in cost efficiency and scale - but this can never be at the expense of security or compliance. And with Solvinity & Azure, it won't.