CSA-CCM SECURITY COMPLIANCE

Secura is your partner for assessing the security of your cloud-based solution. Our assessments based on the CSA Cloud Control Matrix involve a combination of audit activities and penetration testing, covering all the security relevant aspects. Our range of services in the scope of cloud security is focused on both cloud clients and Cloud Service Providers.

IN CONTROL WITH SECURA

Secura has worked in information security and privacy for nearly two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

STATE-OF-THE-ART COMPLIANCE FOR YOUR CLOUD BASED SOLUTION

Cloud solutions are nowadays everywhere. More and more companies are choosing for Cloud First strategy to gain control over their ICT services and to get low cost based access to all kinds of new products and services. However, moving to the cloud does not dismiss you from all responsibilities involved. You need to stay in control over the service delivery and processing performed by your Cloud Service provider (CSP).

Customers of CSPs need to define minimal security requirements for their CSPs and take responsibility for the user control part in their own organization. CSPs need to be in control over their security risks by building, implementing and maintaining a sufficient security control framework. Independent auditors could assess these implemented controls and report on that to prove the existence and effectiveness of these controls towards the CSP, customer and other stakeholders.

All of these involved parties need a standard, a widely accepted and used framework for governance, implementation and audit. Therefore, we advise to use the CSA-CCM (Cloud Security Alliance- Cloud Control Matrix), the first ever baseline control framework specifically designed for managing risk in the Cloud Supply Chain. It describes best the objectives and it is adopted by the ISACA (largest international audit organization) as well as many other institutions. Moreover, the CCM provides a mapping with a long list of other standards and frameworks therefore making it applicable to use as a multi-compliant framework.

OVERVIEW OF THE ASSESSMENT FRAMEWORK

Secura is actively involved in the CSA. The CSA is a not for profit organization whose mission it is to contribute to securing cloud services. We use the CSA-CCM for several purposes. The framework itself is developed based upon the CSA security guide and part of the GRC stack of the CSA. This guide uses the architecture of the NIST for cloud services, determines the risks involved and describes the relevant objectives and controls that could support the involved parties for staying in control over the cloud services. The latest version 3.0.1 of the CSA-CCM is built around 13 domains and 133 controls, mapped to a long range of other industry standards. These controls are applicable for selecting CSPs, implementing supply chain management, assessing the CSP and even auditing them as a guarantee that they comply with a sufficient level of control over their services.

IN CONTROL WITH SECURA

Secura has worked in information security and privacy for over 15 years. By leveraging our experience and expertise, we are a strong partner to address your information security matters efficiently and thoroughly.

Secura can be your partner for assessing the security of your cloud-based solution. Our assessments based on the CSA Cloud Control Matrix involve a combination of audit activities and penetration testing, covering all the security relevant aspects.

Our range of services in the scope of cloud security is focused on both cloud clients and Cloud Service Providers.

For cloud clients

- Support in developing Cloud (security) strategies and policies;
- Support in selecting a CSP using the CAIQ of the CSA that is derived from the CSA-CCM;
- Support in designing and implementing the user control part of the CCM controls;
- Assessments and assurance investigations regarding the implementation of cloud controls in the organization;

For CSPs

- Assessments and assurance investigations using the CSA-CCM as baseline for determining the relevant criteria and controls that need to be tested.

SUPPORT FOR CLOUD CLIENTS

Developing Cloud strategies and policies and implementing the relevant controls in the organization is not always an easy task. At the same time, these steps are critical when you are choosing CSPs and agree upon terms, conditions and procedures to which those CSPs should comply.

Our Cloud security experts can support you using the CSA-CCM and the Consensus Assessments Initiative Questionnaire (CAIQ), also published by the CSA. The answers received to the tailored CAIQ will provide you a strong base for selecting the best CSP to support your solution in compliance with your security objectives.

Furthermore, our certified IT Auditors can provide you implementation support, as well as assurance investigations regarding the cloud controls in your organization, taking the CSA-CCM as starting point.

SUPPORT FOR CSPs

Cloud services are becoming more critical for organizations every day. Trust between parties needs a more solid statement about control as organizations

are depending on those services. Proving the security level increases trust. An assurance investigation by an independent, trusted and qualified third party will deliver this proof. Furthermore, such an investigation supplies the CSP with an expert opinion and recommendations to improve the level of control.

Assurance Service description

There are two variants of assurance investigations. The first on is the Direct version. Secura performs an assurance investigation, including the test work and reports the findings including the opinion. The second one is the Attest version. The CSP then describes its control framework including verifying the existence of those controls and formulates its 'in control' statement. We as the auditor then verify the correctness of the statements and the test results by testing ourselves as well. For these two variants there exist two types of assessments. Type One covers auditing the design and verifying the existence of relevant controls. Type Two covers auditing the design and testing the effectiveness of controls during a certain period.

Process flow

The assurance investigation starts with the engagement and defining of the scope of the investigation. Based upon the cloud architecture and service description we determine the subject of the audit and the controls (objectives) that need to be assessed. Moreover, we identify the relevant shareholders. After understanding the services and architecture we assess the risks involved and plan the audit work.

The findings from our audit will be verified with the auditee before they are reported. After receiving the conformation about the findings we issue the final Assurance Report including our opinion. The Assurance Report is devised in line with internationally recognized assurance standards such as ISAE 3000, offering you an independent qualified opinion for proving your cloud security, according internationally recognized audit standards.

Added value to your business

With our report, CSPs can convince their (potential) customers about the implementation of relevant controls and quality level in their organization while the customers have a qualified opinion about the control level of the CSP they are dependent on. Additionally, the report provides a list of specific user controls that customers themselves need to implement to stay in control.
The audit report can be a considerable step forward to even other certifications like the Cloud Security Alliance STAR Certification.

INTERESTED?
Would you like to learn more about our services?
Please do not hesitate to contact us.

Follow us on

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)40 23 77 990
E info@secura.com
W www.secura.com