CYBERSECURITY ASSURANCE SERVICES

Secura is your trusted partner for providing assurance on your procedures or product security controls. We provide a complete portfolio of services, including:

- *Guidance on how to select the most relevant assessment criteria for the assurance service;*
- *Assessments conducted by experienced auditors, based on the selected criteria;*
- *Writing and signing off the assurance report, the proof of your compliance.*

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.

RECOGNIZED CYBERSECURITY ASSURANCE FOR PRODUCTS AND SERVICES

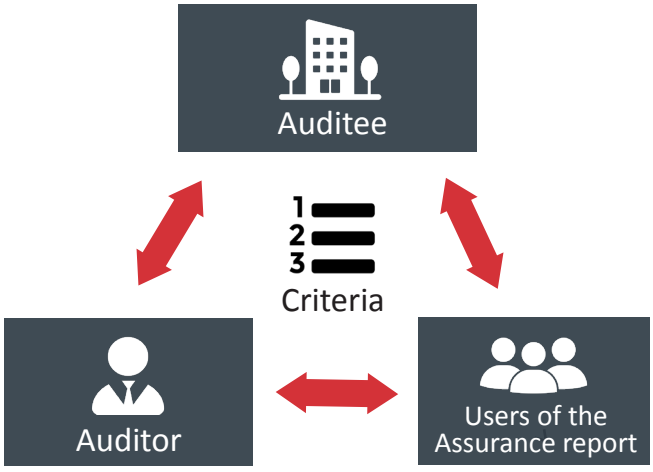
Cybersecurity compliance is an increasingly important process that different actors across various vertical industries are looking for. Compliance can be determined by verifying and testing procedures, policies or product specific security controls against legislation, international accepted frameworks and/or requirements as a result of a security risk analysis. **Assurance services** are professional assessment services that perform audits according to international accepted assurance audit standards, such as **ISAE 3000**. The delivered **Assurance Report** could provide you with international recognition of the security status of your organization or developed products. That makes a difference! Furthermore, you receive an independent qualified opinion of an expert that helps you to improve your security level in the organization, for your products and/or your services.

The Assurance Report describes the results of the cybersecurity investigation and draws conclusions regarding compliance with the considered set of criteria. Assurance Reports are signed off by a certified auditor which confers them more international recognition. Secura believes that providing an independent qualified opinion of an expert gives comfort for the involved people and organizations, proves compliance and addresses shortcomings or considers points for improvement.

ACTORS INVOLVED IN AN ASSURANCE SERVICE

An assurance service requires the following parties for its execution:

- **Client**: The entity requesting the assurance service focused on a particular entity under its management
- **Auditee**: The entity which will be the focus of the assessment. This entity needs to comply with a set of pre-agreed requirements in order to demonstrate compliance
- **Auditor**: The entity performing the assurance service, finally delivering the Assurance Report to the client
- **User**: The entity which relies on the results of the Assurance Report, by making use of the facilities offered by the client



TYPES OF ASSURANCE REPORTS

Depending on the depth of the assessment, assurance reports can be split into:

- **Type I**: A Type I Assurance Report will provide assurance on the general suitability of the design and the existence of security controls according to the identified criteria.
- **Type II**: A Type II Assurance Report will provide an opinion about the design and security controls during a certain period.

ASSURANCE SERVICES DOMAINS AND CRITERIA

An assurance service, finalized with an Assurance Report, can be devised at a very wide range of target products and services, from various domains. Examples of possible evaluation targets are:

1. Information security management systems for organizations in healthcare, industry, banking, government, etc.
2. Cloud hosting and processing facilities
3. Physical devices, such as medical devices, IoT products, ICS/SCADA systems and components, etc.
4. Operating systems and various types of software applications involved in the secure handling of information

One of the most important aspects of an assurance service is the correct identification and definition of assessment criteria. Depending on the assessment domain and target, the relevant criteria can vary a lot. Examples of possible criteria, based on which assessment requirements are derived are:

- National or international standards on information security management (e.g. ISO 27001)
- Frameworks defining controls for improving the security of organizations (e.g. NIST Cybersecurity Framework, NIST SP 800-53)
- Standards and frameworks defining requirements for particular products or process (e.g. IEC 62443 for security of ICS systems, ISO 14971 for risk management on medical devices, IOT Security Foundation Compliance Framework for consumer IOT products)
- Frameworks defining controls for cloud services (e.g. Cloud Security Alliance Cloud Control Matrix)
- Frameworks defining controls related to privacy of user data (e.g. NOREA Privacy Control Framework)

Regular assurance services are:

- ENSIA
- DigiD
- SOC 1
- SOC 2
- Richtlijn 3402
- Privacy Audit Prooftm
- TPM
- Suwinet
- VIPP

We also perform Richtlijn 3000 Assurance engagements covering a.o. software (development) quality, information security, cybersecurity, privacy compliance, baselines information security compliance.

IN CONTROL WITH SECURA

Secura has worked in information security and privacy for over 18 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 trusted partner for providing assurance on your procedures or product security controls. We can provide a complete portfolio of services, including:

- Guidance on how to select the most relevant assessment criteria for the assurance service;
- Assessments conducted by experienced auditors, based on the selected criteria;
- Writing and signing off the assurance report, the proof of your compliance.

ASSURANCE SERVICES PROCESS

By partnering with Secura for an assurance assessment, you are guaranteed to receive a complete evaluation service, based on state-of-the-art criteria. The overview of the process is described in the diagram.

1. Selecting the best assessment criteria (Prepare)

An Assurance investigation follows a standard process, starting with a preparation phase to finalize scope and applicable criteria. We work with you in selecting the best assessment criteria, tailored for your specific use case, as well as your users' interests. Furthermore, communication with and preparation of the auditee, responsible for the subject of matter, is an important aspect of the Prepare phase.

2. Performing the audit (Execute)

In the Execute phase we perform our audit work. Our team is built on expertise and experience relevant for the engagement. The findings are verified with the auditee and reviews are done to guarantee the quality of work.

3. Deliverables (Report and Evaluate)

In the Report phase we write the Assurance report type I or II according to the requirements of the audit standards. A draft version is usually checked with the client or responsible employee. After receiving the confirmation letter we publish the final report. The engagement is than completed with an evaluation where we discuss the process, outcome and relevant best practices to follow-up findings.

4. Our value to you

The delivered Assurance report could provide you with international recognition of the security status of your organization or developed products. That makes a difference! Furthermore, you receive an independent qualified opinion of an expert that helps you to improve your security level in the organization, for your products and/or your services.

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