Cyber Security Assessment

Do not give hackers a chance and minimise your cyber risks. A security assessment helps you to detect possible vulnerabilities in your company quickly as well as identify and reduce the risks.

Swisscom analyses the security in your company, identifies the cyber risks and supports you in the development of suitable measures.
The security assessment by Swisscom includes a range of services for examining the organisational and technical security controls in your company and identifies

their vulnerabilities. You obtain an individual assessment from security experts. Moreover, you learn how you can minimise potential risks in your company and also prepare for the dangers of tomorrow.

Your benefits with a security assessment

Independent and thorough assessment

You discover the potential ICT risks in your company and learn how to minimise them.

Proactive verification, evaluation and elimination of vulnerabilities

Protective activities can be prioritised based on the vulnerabilities found. This gives you the advantage of actively tackling vulnerabilities and achieving more efficient results. This means your budget can also be allocated more effectively.
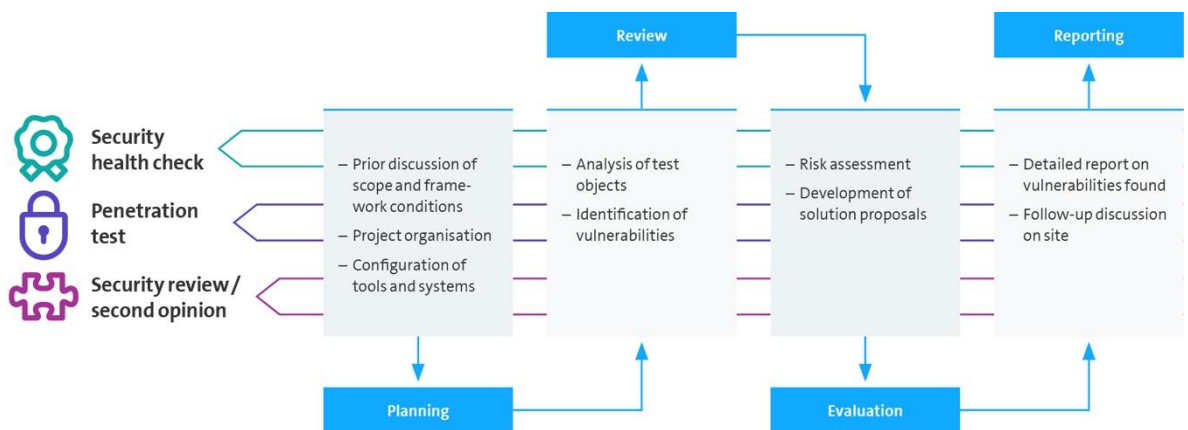
Investment planning

The results provide a basis for decision making on possible optimisations and the implementation of further projects.

The approach of security assessments

swisscom

Facts & Figures

The security health check provides an ideal assessment and reveals strengths and weaknesses in information security in your company. The necessary information is obtained using an information security questionnaire based on ISO standard 27002 and other recommendations. By performing an individual technical assessment, Swisscom identifies the systems in your network and examines them for known vulnerabilities and possible configuration errors. Vulnerabilities are subjected to a risk assessment.

Security health check

Content
– Multi-day semi-automated examination of selected test objects by specialists on site
– Interview-based information gathering on site
– Solution proposals with specific measures
– Report and final presentation

Result
The summary of results, risk assessment and recommendations for action are presented to business and IT management. A detailed final report and the presentation are made available electronically.

You obtain a realistic assessment of how resilient your IT is against malicious attacks. From the perspective of an internal or external attacker, Swisscom checks an application defined by you, a system or an entire infrastructure for weaknesses and security vulnerabilities.

Penetration test

Content
– Internal or external penetration test following the blackbox or whitebox approach
– Individual examination of defined test objects (web applications, ICT systems, IoT devices, etc.) by proven experts
– Identification and targeted exploitation of vulnerabilities
– Report and final presentation

Result
A technical detailed report indicating all known vulnerabilities and their effective countermeasures.

Swisscom offers you an impartial second opinion on system designs, security plans, configurations as well as security requirements. Swisscom also offers support in the development and implementation of security measures.

Security review and second opinion

Content
– Analysis of existing solutions or plans and preparation of a risk matrix
– Definition of measures to reduce risks to an acceptable level
– Implementation of measures to reduce residual risks
– Reporting

Result
The result is a report on the defined test object that ascertains the overall security, identifies and assesses vulnerabilities, and presents potential for improvements.

You can find more information and the contact details of our experts at swisscom.ch/security-consulting

swisscom