Don't give hackers a chance and minimise your cyber-risks. A security assessment will help you quickly identify possible weaknesses in your company, and assess and minimise the risks.

Swisscom can analyse your company's security, identify cyber-risks and help you devise suitable measures.

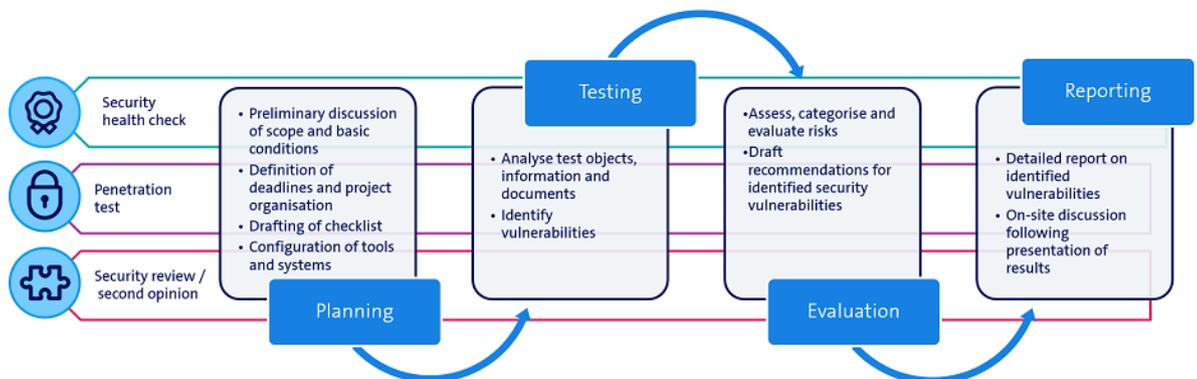### What is Cyber Security Assessment?

Swisscom's security assessment comprises various services designed to assess your company's organisational and technical security controls and identify their vulnerabilities. You will receive an individual assessment from security experts. You will also learn how you can minimise potential risks in your company and, at the same time, protect yourself against future dangers.

Your benefits with a security assessment

‒ Independent, thorough analysis
You will be made aware of potential ICT vulnerabilities in your company and how to minimise them.

‒ Proactive verification, evaluation and correction of vulnerabilities
On the basis of identified weaknesses, protection activities can be prioritised. This gives you the advantage of being able to address vulnerabilities proactively and thereby achieve more efficient results. The budget can then also be allocated more effectively.

‒ Investment planning
The results can serve as the basis for decisions on possible improvements and future projects.

Our security assessment procedure

Facts & Figures

Security health check

Description	The security health check provides a detailed review of your current situation, showing the strengths and weaknesses of information security in your company. The required information is gathered using an information security questionnaire based on the ISO 27002 standard and other recommendations. With an individual technical assessment, we can identify the systems in your network and check them for known vulnerabilities and possible configuration errors. Vulnerabilities are subjected to a risk assessment.
Content	– Semi-automated analysis of selected test objects by on-site specialists over several days – Interview-based information gathering on site – Recommendations with practical measures – Report and final presentation
Result	The results summary, risk assessment and recommendations for action are presented to the company's senior and IT managers. A detailed final report and the presentation are made available electronically.

Penetration test

Description	You receive a realistic assessment of your IT's ability to withstand malicious attacks. From the viewpoint of an internal or external attacker, we examine an application, system or entire infrastructure selected by you for weaknesses and security vulnerabilities.
Content	– Internal or external penetration test according to black-box or white-box approach – Individual testing of defined test objects (web applications, ICT systems, IoT devices, etc.) by proven experts – Identification and deliberate exploitation of vulnerabilities – Report and final presentation
Result	A detailed technical report, mentioning all identified vulnerabilities and effective counter-measures.

Security review and second opinion

Description	We give you an independent second opinion on system designs, security concepts, configurations or security guidelines. We also help you to develop and implement security measures.
Content	– Analysis of existing solutions or concepts and creation of a risk matrix – Definition of measures to reduce risks in a specific field – Implementation of measures to reduce residual risks – Reporting
Result	The result is a report on the defined test object, containing information on security as a whole, identifying and evaluating weaknesses, and describing potential improvements.

You can find more information and our experts' contact details at: **www.swisscom.ch/security-consulting**

swisscom