



Consulting Services 12-1: ICT Security Assessment



Information is a valuable asset that has to be appropriately protected for each organisation. In an “ICT Security Assessment” an impartial outside expert determines and evaluates the current ICT situation, giving special attention to information security. The assessment centres on the technical infrastructure and on the processes and responsibilities currently in place and used in an organisation.

The “ICT Security Assessment Package” entails an evaluation and assessment by experts from Crypto AG. The results are compared with best practice standards as a benchmark. Where required, Crypto AG then makes suggestions on how to mitigate or avoid the biggest risks.

An ICT security assessment alone does nothing to increase information security, but it does indicate the status quo of an organisation and points out where action is needed to improve information security. Technical and organisational actions may be suggested to mitigate or avoid detected risks, if need be. The analysis proceeds on the following levels.

Organisation: Experts check the efficiency of the protective measures in place. The object is to pinpoint the weakest link in a complex networked environment and render security measurable and controllable. Experts from Crypto AG compare the precautions you take with best practice standards using ISO 27001, ISO 13335, COBIT, ITIL, etc. as references and benchmarks.

Technology: Technical measures are deemed extremely effective and appropriate if applied correctly. Experts from Crypto AG examine and evaluate the implemented technology and the effectiveness of the protection systems already selected.

Processes and people: Technology alone cannot guarantee information security. Other major factors are the operating processes in place within your organisation and the associated roles and responsibilities. These too are considered and rated in the assessment.

Not least, the assessment findings and recommendations can be used as justifications for investments in information security.

Key Benefits

- Examination of the efficiency of the protective measures that are planned or implemented
- Expert opinion from an impartial outside party on the current level of information security and any existing weaknesses
- Justification for investments in information security
- Security is rendered measurable and as such, can be controlled and monitored
- Basis for making decisions in the evaluation phase
- Action plan for your organisation with respect to information security

Description of service

Crypto AG supplies the knowledge, experience and procedures on how an organisation can conduct a risk assessment and compares the status quo with best practice standards. Proposals are drawn up for the five major identified ICT security risks to point out how they can be mitigated or avoided. As an alternative, risk can also be borne or passed on. The findings are prepared to give decision-makers at your organisation useful information for determining what degree of information security should be put in place.

Glossary

COBIT: Control Objectives for Information and related Technology (COBIT®) is a Control Framework of the ISACA

ISACA: Information Systems Audit and Control Association (ISACA) is the professional association for IT auditors

ITIL: IT Infrastructure Library, in the meantime also released as ISO 20000

ISO/IEC: International Standardisation Organisation / International Electrotechnical Commission

ISO 27001: Information technology — security techniques — information security management systems — requirements

ISO 13335: Information technology — security techniques — management of information and communications technology security

ICT: Information and communication technology

Deliverables

Crypto AG evaluates the currently implemented ICT security system (determination of the status quo) and compares it with best practice approaches. The following documents are produced:

- Evaluation of the situation as regards applicable standards
- Analysis of the physical and technical security in a workshop and a review
- Analysis and evaluation of the processes and responsibilities
- Assessment of the level of security at your organisation (benchmark)
- Presentation of results and risk assessment
- Suggestions on how to improve the situation with regard to the five biggest risks

Details

Kick-off Meeting: At the kick-off meeting, the procedure is explained to you, and the scope of activities and deadlines are agreed.

Policy review: First, the standards applied in the organisation are determined along with the method used for classifying data considered worthy of protection.

Technical review: Next, the physical and technical precautions taken are examined, tested and assessed.

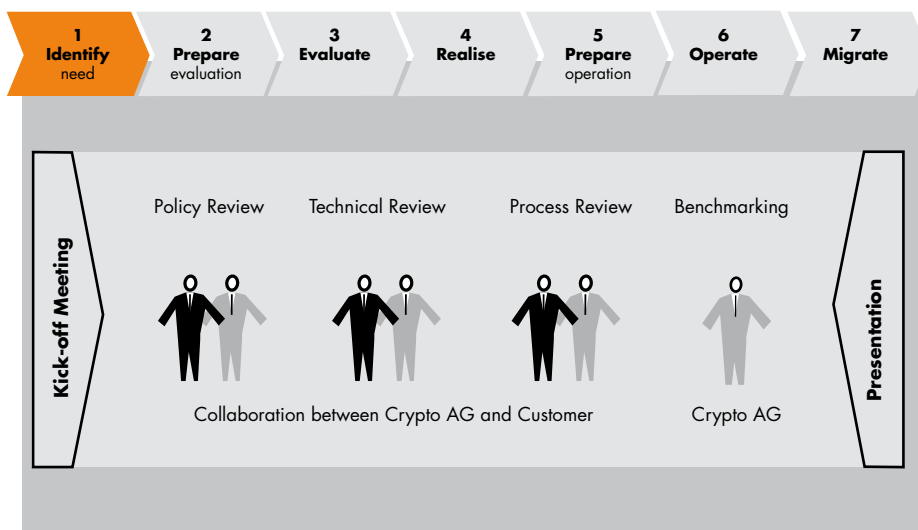
Process review: Technology alone cannot effectively protect valuable information. An organisation has no management system for information security until three criteria are met: Formalised processes must be put in place, the operating personnel must be familiar with these processes and apply them, and clear-cut roles and responsibilities must be defined and implemented.

Risk assessment and benchmarking: Experts from Crypto AG assess the situation and compare it with best practices as laid down in standards such as ISO 27001, ISO 13335, Cobit and ITIL.

Options:

- Information Security Awareness Workshop, where the key principles of information security are explained
- Preliminary meeting to discuss the results at Crypto AG in Switzerland, including implementation examples

Interaction with Crypto AG



Related services

- 13-1 ICT Security Architecture & Concepts
- 51-1 ICT Security Process Framework