



## Consulting Services 51-1: ICT Security Process Framework



**Tasks and processes can only be done at a consistent level of quality if they are formalised. This fact is well accepted. The same arguments that led to process-oriented quality management also apply to information security. Although certainly important, the technology used does not suffice to ensure a defined degree of information security. This high level of information security cannot be established and kept traceable in the long term until formalised processes and clearly defined responsibilities are put in place.**

**The “ICT Security Process Framework Package” adapts the most important processes for information security to your situation and environment based on best practice standards.**

The process framework follows the top-down approach. This means clear guidelines on information security must be formulated at the strategic level of an organisation in a security policy. These guidelines are then implemented at other levels. For instance, decisions on who implements what is made at the tactical level using concept papers and standards. Implementation for each unit is then ensured at the operational level. However, all these efforts do not add up to a management system until implementation is measured, experiences and changes are taken into account and compensated for in a continual improvement process.

A properly focused management system is required to keep information security at a high level throughout the entire lifecycle of a solution. Various well known best practice approaches such as ITIL, COBIT, COSO, ISO 27001, and ISO 13335 are all in agreement on this point. The objective of these approaches is to have a management system protect confidential information in defined and traceable processes.

### Key Benefits

- Best practice processes adapted specifically to your needs
- Optimised operation of security infrastructure can be controlled
- Compliance with internal and external security requirements
- Effectiveness of information security within your organisation can be measured
- Security problems are detected and solved quickly
- All security incidents/logs are stored in a central place
- Clearly defined roles and responsibilities in the operating organisation

## Description of service

Crypto AG supplies the knowledge, experience and procedures on how security processes and responsibilities can be adapted to create a customer-specific process framework based on best practice approaches. Processes are defined to fit your needs, infrastructure and environment, so that the degree of information security defined in your security policy can be maintained for the long term and can be constantly monitored.

## Deliverables

Together with your experts and operating managers, Crypto AG defines a formal process framework tailored to your individual needs. In the process, best practice approaches are adapted for the following security aspects of your operating organisation:

- Encryption key management
- Device and configuration management
- Incident and problem management
- Change management

## Details

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

**Assessment:** First, it is determined which guidelines are already in place in your organisation and which formal process descriptions exist.

**Process framework design:** Then, your specific scenarios are determined and combined with the already existing guidelines and best practices to create a formal process framework.

**Process framework adaption:** Next, the process framework is adapted to existing roles and responsibilities and to the people involved. Interfaces with other processes may also be considered and adapted, where appropriate.

### Options:

- Information Security Awareness Workshop, where the key principles of information security are explained
- Assistance with implementing the process framework

## 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 27001:** Information technology — security techniques — information security management systems — requirements

**Encryption key management:** Processes and responsibilities for creating and distributing customer-managed parameters (CMP) and all other security parameters for encryption

**Device and configuration management:** Processes and responsibilities for the central management of all equipment, licences, serial numbers and versions of the components that are used and that make up the security infrastructure

**Incident and problem management:** Central reporting point for handling all security incidents, complete with escalation and clear-cut responsibilities. The security level is monitored and messages are accepted

**Change management:** Formal process for documenting, approving, testing and implementing changes to security systems

## Related Services

- 12-1 ICT Security Assessment
- 13-1 ICT Security Architecture & Concepts

## Interaction with Crypto AG

