

Maintaining IT-Security

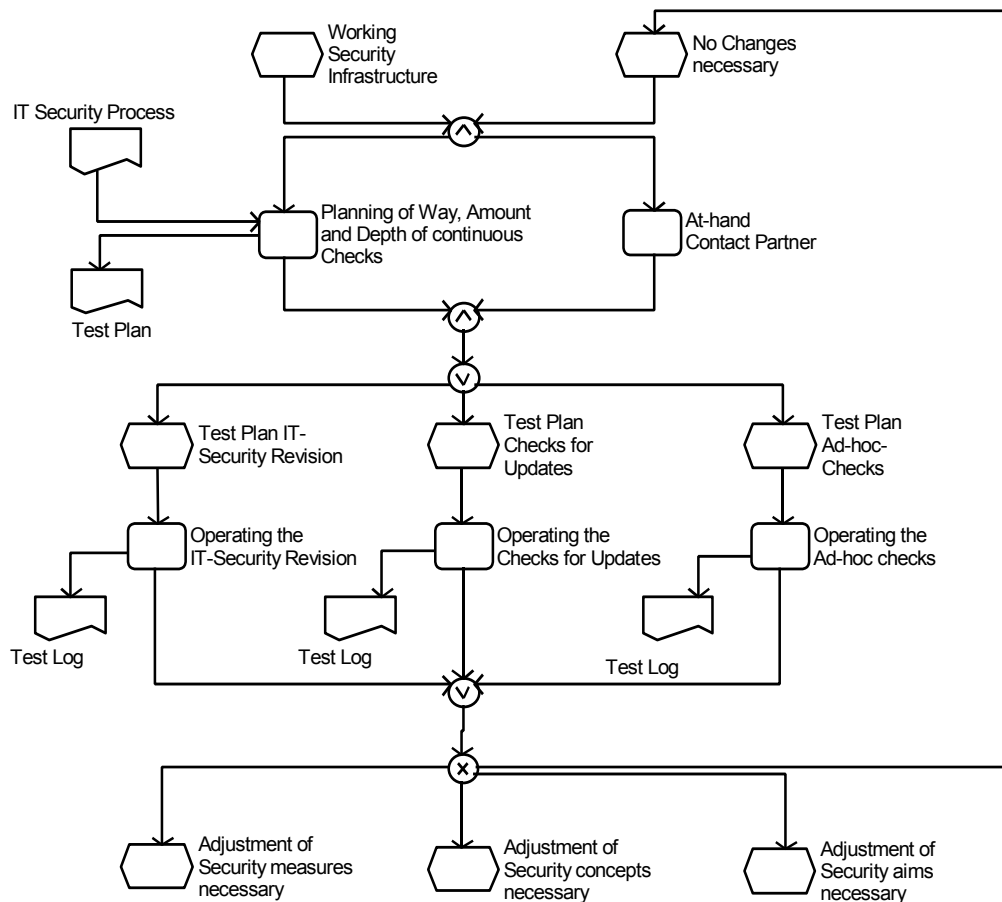


Figure 9: Maintaining IT-Security

This sub-process comprises only the description of the technical examination of the IT-Security. In conjunction with other sub-processes of the first section of the reference-process, overall IT-Security is established. This includes participating in the process of the negotiation of contract terms, developing security awareness among various actors and co-operating with the partners.

The directions of the BSI-Grundschutzhandbuch M 2.199 (Federal Legal Reference) are relevant especially for the maintenance of the IT-Security.

Actions: Maintaining IT-Security

- Planning of way, amount and depth of continuous checks of the present IT-Security infrastructure
- Being available as a contact partner for security-relevant questions and directions
- Operating IT-Security revisions
- Operating checks for updates
- Operating ad-hoc checks in case of (potentially) security-relevant directions or incidents

Fields of competence: Maintaining IT-Security

Competencies/Ability to:

- Translate criteria of security, duty of secrecy (data protection), progress and failure as well as respective problem specifications into measurable parameters and testable criteria
- Derive assessment criteria
- Know and recognise special risks
- Apply legal foundations and rules concerning IT-Security and the duty of secrecy (data protection)
- Draw up examination plans including time, content, milestones etc. for different areas and tasks
- Synchronise singular plans to a plan as a whole
- Choose and operate automatic observation tools
- Adequately communicate with different colleagues of the company (address, media of communication, behaviour)
- Estimate the relevance of reported security-relevant incidents
- Have informal conversations with colleagues to build up and maintain mutual trust
- Set up and look after open (if need be anonymous) communication opportunities, e.g. security consultation-hour, web-forum in the company-intranet etc.
- Analyse and interpret logfiles and messages from observation tools and to initiate appropriate measures
- Operate security revisions and updating checks if need be in co-operation with the appropriate authority (e.g. administrator)
- Document and record security revisions and updating checks as well as ad-hoc examinations
- Evaluate check results and consider their relevance for security

Knowledge

- Immediate utilisation of security- and data protection-relevant regulations, norms and standards in the company
- Level of security, security measures and security infrastructure of the company
- IT-security and protection measures, their mode of operation, tasks and risks
- Data protection measures, their mode of operation, tasks and risks
- Information retrieval about current security-relevant incidents (mailing-lists, security advisories, bug reports etc.) and protection measures
- Risks of and for IT-systems
- Communication models
- Components and rules of verbal and nonverbal communication
- Representative communication patterns and their appropriate utilisation
- Characteristic conflicts, their cause and symptoms
- Test plans and their design
- Techniques and methods to test and observe IT-systems and their risks

Tools/Methods

- Monitoring tools
- Data flow and data management

Example: Maintaining IT-Security

After having gone live, checks for maintaining IT-Security take place at certain intervals, following system and network upgrades, migration to new technologies, after joining new networks or plugging into internet, intranet or extranet, or following the installation of new basis software.

In the actual example, an automatised Managed Vulnerability Assessment Tool was implemented. This tool periodically checks the security of public access systems as well as a number of internal systems.

On the basis of this, the IT Security Coordinator obtains analyses and detailed indications on how to find and eliminate weak spots.