InfoGuard
SWISS CYBER SECURITY

SOCIAL ENGINEERING AUDIT

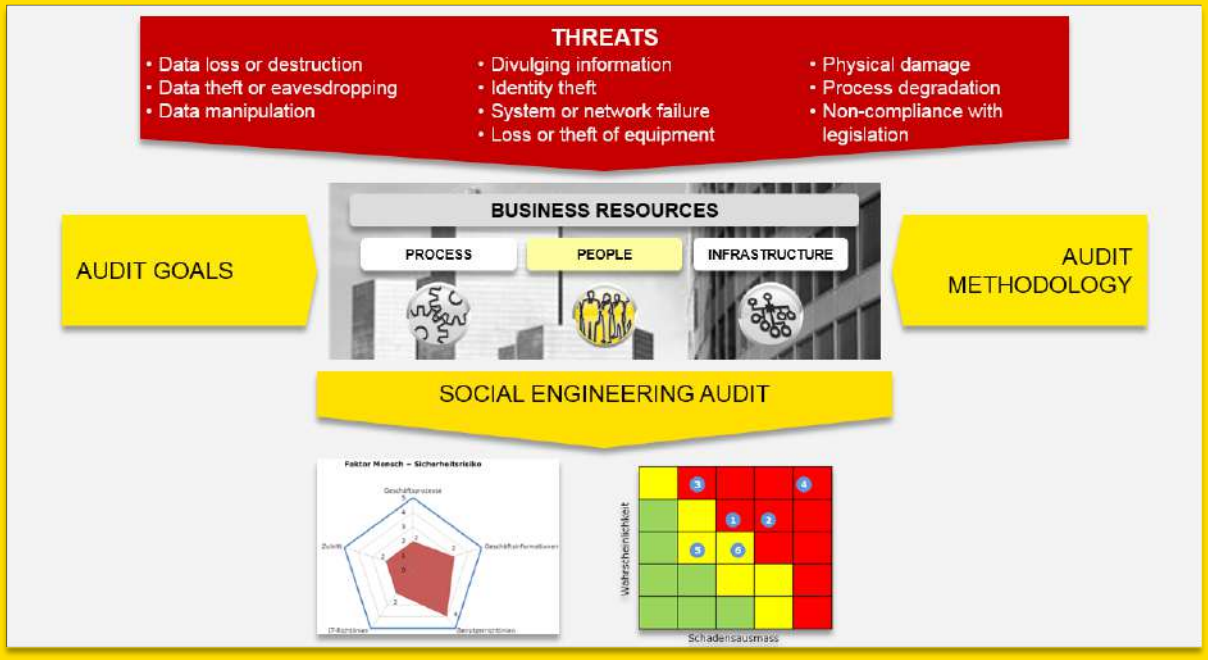
The «human» risk factor systematically examined.

VERIFYING YOUR EMPLOYEES' SECURITY AWARENESS

Our social engineering audits are not about scrutinising individuals; rather we run anonymous checks of compliance with security-relevant business processes and guidelines, and of the handling of sensitive information. All audit objectives and methods are discussed in advance with the client before being authorized by the security officers.

Depending upon the aim of the audit and the target group, we adopt different social engineering audit methods and attacks, ranging from direct contact, either by telephone or in person, to electronic channels, such as email, chat or social network platforms, up to postal contact with the target. Where required, we also add the selective handing over of manipulated USB storage media, the systematic data analysis over the Internet, or the evaluation of log files and system information to InfoGuard's attack repertoire.

- **Identify weaknesses in handling sensitive business information.**
- **Selective investigation of compliance with security-relevant business processes, user guidelines, IT security directives and access guidelines.**
- **Define a profile of strengths and weaknesses vs. the ISO 27002, and describe specific measures to minimise risk.**



Audit goals

- Security-relevant business processes
- Handling sensitive business information
- Compliance with IT security guidelines
- Compliance with access guidelines

Audit methods

- Information gathering
- Personal contact
- Interviews
- Phishing and malware
- Analysis of IT systems
- On-site inspections

Communication paths

- Personal interview
- Letter
- Telephone and SMS
- Email and Internet
- Social Network platforms

Systematic approach starting with a threat analysis, continuing with planning and implementation and ending with a risk assessment and recommendation of actions to be taken.

Social Engineering Audit in six steps

1 Threat analysis and definition of the audit goals
The basis for the examination is given by a specific threat analysis with the dangers, chances of success and risk classes. We look at risks the likes of data loss, theft and manipulation, identity theft and breach of company-internal processes or legal provisions, to name just a few. In a kick-off meeting, together with the client, we define the aims of the audit, we make an appointment for the attacks, and we clarify responsibilities and framework conditions.

2 Planning the assessment, and review of the audit methodology
In this project step we examine the client's relevant user directives and available security baselines. To find out what is allowed, and what is not, we analyse the existing guidelines and conduct additional interviews. The most effective audit methods are then described, planned and recorded in a detailed script, which is then examined and approved by a responsible person appointed by the client.

3 Assessment
The key phase is now the execution of the assessment itself, using the previously defined tests. This step is always a combination of different audit methods. Should serious shortcomings be identified, the client is immediately informed, so that the required adaptions can be put in place without delay.

4 Workshop – Risk evaluation
The results of the assessment are discussed with the client in a workshop. The identified weaknesses and the main risks surrounding information security, in particular the 'human' factor, are interpreted and evaluated so that the report can finalised.

5 Report with an evaluation and recommendations
All the findings resulting from the analysis and the workshop are listed in the overall report, represented in a profile of strengths and weaknesses, and compared on these grounds with the international standard for IT security ISO 27001. The identified weaknesses are rated, and accompanied by recommendations. The specific recommendations, with regard to actions to be taken, are described in detail and prioritised on the basis of the risk assessment.

6 Closing meeting
The final report is presented to, and discussed with the client. A comprehensive and significant summary is created for the management, describing the implementation of the project, the results of the survey, and the resulting security measures. It goes without saying that we remain available to assist the client with the implementation of the required countermeasures, should the need arise.

SOCIAL ENGINEERING AUDIT – ONLY ONE ELEMENT OF COMPREHENSIVE SECURITY AUDITS AND REVIEWS

Your business processes can only function properly if the correct information is in the right place at the right time. Confidentiality, integrity and availability of information play a significant role.

InfoGuard offers an independent assessment of your information security. We show you which organisational, technical and personnel weaknesses are manifest in your company and how you can counteract them.

Our services embrace the following areas:

- Security Audit based on ISO 27001/27002
- Gap analysis in view of an ISO 27001 certification
- System and architecture review
- Penetration test based on OSSTMM
- Vulnerability scan
- Social Engineering Audit

Your security is our goal –
we analyse and optimise your security system!

InfoGuard – The Swiss Cyber Security Expert

InfoGuard is the Swiss expert for comprehensive cyber security and innovative network solutions. You can benefit from our experience, professionalism and reliability in the auditing, consultation, architecture and integration of leading network and security solutions. We deliver state-of-the-art cloud, managed and cyber defence services from our ISO 27001-certified InfoGuard Cyber Defence Center located in Switzerland.

InfoGuard AG
Lindenstrasse 10
6340 Baar / Switzerland
Phone +41 41 749 19 00

Office Bern
Stauffacherstrasse 141
3014 Bern / Switzerland
Phone +41 31 556 19 00

INFOGUARD.CH