



**“People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.”**  
— Bruce Schneier

## Social Engineering Testing

***Security systems have certainly been greatly improved in the last couple of years. However they all continue to share a common weakness: They depend on humans to function properly. This universal characteristic happens to be their most significant flaw, as the human element of security is often easily subverted.***

### Risk Management Framework



Risk management is the ongoing process of identifying risks and implementing plans to address them. Risk is determined by considering the likelihood that known threats will exploit valuable assets and the impact if an exploit is successful. It is very important to know where to apply available resources to mitigate risk in an efficient and cost-effective manner. That's where risk assessments come in the picture. Risk assessment is the part of the ongoing risk management process that assigns relative priorities for mitigation plans and implementation.

### Ascure Assessment Program

Ascure's Assessment Program situated in Step 4. Assess Controls. Ascure performs activities in all 6 steps of the risk management framework and can help in implementing such a framework within your company.

This program has 4 pillars:

- Logical tests
- Physical tests
- Social tests
- Strategic tests

Logical testing concerns everything on the network, system and application layer. This includes intrusion testing (external, internal, web applications, database systems...), system auditing (servers, workstations, network components...), code reviews, architecture reviews.

### About Ascure

Ascure is specialized in operational risk management consultancy and staffing. Operational risk management, information security, business continuity and compliance to laws and regulations are major cornerstones of our services.

Ascure assists its customers with the incorporation of operational risk management at all levels and in all areas of their organization, including day-to-day operational decisions. No decision should be taken in any organization without applying proper operational risk management. It can be applied throughout the entire life cycle of any activity or project. In order to minimize risk, it is however preferable to apply operational risk management at the beginning phase of a project or operational activity.

### About Ascure Academy

Ascure offers an extensive education and awareness program through the Ascure Academy which covers several open classes, events and customized education experiences.

### Contact

For further and additional information, please contact us on Tel. +32 (0)9 243 10 20 or [info@ascure.com](mailto:info@ascure.com)

Ascure's general terms of delivery are applicable to all our services.

In physical and social tests we try to exploit the human factor to gain access to your information and/or your network.

Strategic tests are higher level tests and can be risk analysis, Business Impact Analyses, High Level Risk Management Audits, Gap analysis between your situation and regulations/standards (ISO27002, CBFA guidelines, PCI...)

We can assist in setting up such an assessment & intrusion program and assisting your Audit department in tackling these different pillars.

### **Identifying Procedural Flaws**

Operational procedures are often based on mutual trust between the parties involved, and have little consideration for handling dishonest participants. This means open opportunities for malevolent individuals to abuse these procedures and gain access to something they shouldn't. Procedures for access management, password resets and building entry should be thoroughly tested for these weaknesses, and this is best done by posing as a malicious individual.

### **Assessing Employee Awareness**

One of the major pillars of security is awareness. Employees are often told to treat external emails with attachments with great care and suspicion, but how about external calls, visitors, service personnel, business events? The only true way of measuring security awareness is by putting it to the test.

### **Measure Response and Escalation**

Response times in incident handling programs are often based on estimation or basic simulation.

To truly know if these values are correct, a number of incidents should be generated where these times can be measured. As the escalation path is seldom known for incidents that don't take place, this should be tested as well. Additionally, as practice makes perfect, this testing will improve the response given to future "real" incidents.

### **Evaluate Efficiency of Controls**

While many security controls sound good on paper, in many cases the human element poses a significant weakness to their effectiveness. Controls such as guards, reception desks registration and social control are often less effective than they are believed to be.

### **Approach**

The following steps will be followed for the testing:

- **Passive Information Gathering:**  
Non-intrusive information gathering, from a remote location (e.g. internet, publications, press releases,...)
- **Active Information Gathering:**  
A more hands-on approach, including on-site observation, dumpster diving, email/phone information gathering.
- **Social Engineering:**  
In this phase we will target sensitive information directly, by coercing people into disclosing it.
- **Physical Intrusion:**  
Gaining access to an organization's premises by controlling the human element of security.
- **Response/Escalation Testing:**  
Deliberately triggering an alarm condition and measuring the response times and escalation path.
- **Company Events:**  
These events are often accompanied by a lower sense of alertness and watchfulness, and thus provide a great opportunity for social engineering.

### **Deliverables**

You will be provided with a comprehensive multi-level reporting ranging from management level to detailed technical level. All discovered issues and weaknesses will be described and discussed in these reports, as well as the possible methods of remediation to mitigate the risk factors. A list of improvement actions which will increase the overall network security level will be included as well.

You will also receive a list of tests that have been performed together with their outcome.

### **Added Values**

Our trained and certified security consultants are specialized in ethical hacking techniques, among which detecting, attacking and exploiting vulnerabilities. We have members in various local security chapters, like OWASP and ISSA.

We strive to deliver complete and accurate, yet understandable reports of the conducted tests. We strongly believe that adopting your business jargon is the best way to assure an unambiguous description of our assessment.

When a social intrusion test is combined with a business impact analysis, we map the detected issues on an estimation of their effect and remediation costs. We can thereby coach you in the selection of the best fitting remediation for the discovered issues.

Aszure's procedures for assessments are based on strict guidelines and methodologies such as OSSTMM, OWASP, ISSAF and the NIST 800-53a and 800-115.

Interested in world-class education and training: visit the website of the Aszure Academy ([www.ascureacademy.eu](http://www.ascureacademy.eu)).

For more information, please contact:

Tel.: +32 (0)9 243 10 20

E-mail: [info@ascure.com](mailto:info@ascure.com) [www.ascure.com](http://www.ascure.com)  
Bijenstraat 16-17, B-9051 Ghent, Belgium

