RISK ASSESSMENT

COMSEC

What is Risk Assessment?

Comsec's risk assessment provides the company's management with a holistic view of the security level of the network/system, presenting the threats and risks to which it is exposed and providing recommendations for mitigating these risks in the most efficient way possible.

Clients Problems

Thousands of security vulnerabilities are discovered every year in software, systems and IT infrastructures. Attackers exploit these vulnerabilities to penetrate the communications networks of organizations and gain access to critical assets for purposes of harming confidentiality, integrity and availability of data or systems. Motives for the attacks vary, and include, among other things, financial, political and competitive motives (e.g. theft of technology) or a desire to cause harm (e.g. by an angry employee).

Because security vulnerabilities can cause great damage, it is essential for companies to identify and remediate them before they can be exploited.

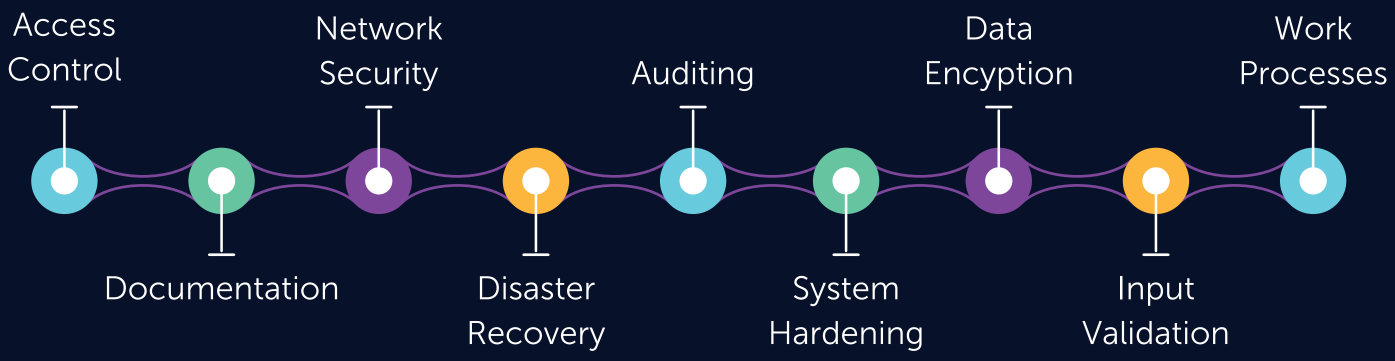
Comsec's Solutions

In order to check the organization's adherence to security best practices and to identify security vulnerabilities, Comsec offers a risk assessment service. This is a security review conducted by leading cyber security experts, which provides a holistic view of the security level of the network/system, presenting the threats and risks to which it is exposed and providing recommendations for mitigating these risks.

The Comsec risk assessment is performed using a white-box security approach in which the organization shares as much information as possible about the internal functionality of the system/network. The information is collected through a series of interviews with key personnel and a set of hands-on configuration tests carried out against components in the network/system to detect security vulnerabilities introduced by misconfigurations, application flows or procedural deficiencies.

Comsec's Risk Assessment

During a risk assessment, the security controls in the following areas are examined in order to identity any security weaknesses that could jeopardize the confidentiality, integrity and availability of the corporate assets:



Access Control

Documentation

Network Security

Disaster Recovery

Auditing

System Hardening

Data Encyption

Input Validation

Work Processes

We then perform a risk level evaluation, during which the impact and likelihood of each vulnerability that has been found is examined in order to determine whether it poses a risk to the organization / system and what the level of that risk is.
The impact grade represents the estimated amount of damage that exploitation of the finding could cause, while the likelihood grade represents the probability of that vulnerability's being exploited. The risk for each finding is calculated based on taking the impact and likelihood grades found and computing the risk level according to the risk matrix used by Comsec or the assessed company.

The final stage of the assessment is the writing of a report. This includes writing an executive summary describing the work that was performed and its main findings, as well as an in-depth description of all of the vulnerabilities that were noted, including an explanation of the potential damage that could result from the exploitation of those vulnerabilities and how likely they are to be exploited.

All findings are rated according to risk and accompanied by a clear set of recommendations for mitigating the finding.

Comsec UK

33rd floor, Euston Tower
286 Euston Road
London, NW1 3DP, England
Tel: +44 (0) 2034638727
info@comsecglobal.com

Comsec BV

Hogehilweg 4
1101 CC Amsterdam
The Netherlands
Tel: +31 (0) 102881010
info@comsecglobal.com

Comsec HQ

Yegia Kapayim St. 21D
P.O.Box 3474, Petach-Tikva
Israel 49130
Tel: +972 (0) 39234646
info@comsecglobal.com

COMSEC