Security Risk Assessment

Security Risk Assessment And Audit

Security risk assessment is a process of identifying, analysing and understanding information assets, possible impact of security risks, weaknesses and threats in order to apply appropriate security measures.

Security Risk Assessment Process

The security risk assessment process generally includes the identification and analysis of:

1. all assets of the system;
2. threats that may affect the system's confidentiality, integrity and availability. For example, the spread of malicious code and unauthorised access to information;
3. system vulnerabilities that are related to the threats, for example, not applying the latest security patches for software;
4. potential impacts, likelihoods and risks caused by threats.;
5. security measures required to control the risks. For example, enhance the protection of network components and equipment, and update the settings of relevant systems; and
6. selection of appropriate security measures and their relationship with the risks.

Security Audit

Security audit is a process in which the organisation's security policy and other security standards are used as the basis to assess whether the overall state of the existing protection measures is up to standard.

Security Audit Process

The procedures of security audit include the following steps:

- Define audit scope – Develop a security audit list covering such domains as Internet application system, network architecture and wireless network.
- Identify security loopholes – Find out all the potential security loopholes using security audit tools and different technologies. For example, Penetration Testing is used to identify possible invasion routes and find out the potential security loopholes and weaknesses of the network and the system.
- Provide recommendations for improvement – After completion of the security audit, an audit report will be compiled for comparing the differences between the existing protection measures and the defined security policy and standards, and subsequestly making recommendations for improvement.