



High Level IT Security Assessment

Nclose offers a "High Level IT Security Assessment" service which is designed to give clients a birds eye view of their IT security posture. This service gives the client the benefit of an outside security review of their environment which analyses and measures their level of security versus industry standards and best practices. This is a high level evaluation and not designed as a replacement for a security audit or vulnerability assessment but rather an exercise to identify and prioritise existing and potential security risks.

Benefits

- Builds a foundation for a company's overall security strategy.
- Identifies risks and vulnerabilities within the company's environment.
- Provides a roadmap to achieving and proactively supporting and maintaining the ideal security posture.
- Low cost and quick turn around times, enable you to have a concise and focused security report with minimal delay and outlay of company resources.

Process

The security assessment consists of approximately 4 to 5 hours on site and 3 to 4 hours off site to analyse data and compile the report. The security assessment consists of three steps namely:

- (1) Information collection – Nclose will meet with staff to discuss existing network architecture, data flows, policies, security controls and administration procedures and any other key topics required to compile the assessment. If the client wishes to focus on any specific area it should be addressed at this stage.
- (2) Data analysis – Detailed analysis is performed of all the data collected. This evaluation takes into consideration existing best practices and industry standards.
- (3) Reporting – Finally, a full report is compiled presenting the findings. Existing weaknesses and strengths are identified with supporting information. Recommendations as to which areas need attention and their priority based on risk are presented, which enables the client to make informed decisions on their security roadmap.

The Result

At the end of the assessment the client will have a clear understanding of where he stands with regards to IT security in his environment. This will enable the client to prioritise the identified weaknesses and form a strategy to address these issues. Below is an example of some of the questions that the assessment will answer:

- Is my perimeter security sufficient to protect my network?
- Does my security policy go into enough detail to protect me as it should?
- In what area should I focus my allocated security resources to in the next six months?
- How can I better use my existing security resources to address my security weaknesses?
- Is my VPN configured in a way that opens my network up to unnecessary risk?
- Are my processes to control software on workstations inline with best practices?

For further information on this service please contact Nclose for a quotation. In addition to this high level assessment, Nclose also offers various other audits, assessments, and tests to ensure your network is as secure as possible.