

Greg

As discussed, the most appropriate next step would be to discuss an initial assessment of your firms existing InfoSec systems.

An Information Security Management System, is an integrated management approach to all aspects of information security. An effective ISMS ensures that both technical and human controls are in place and operating. The ISO/IEC 27001:2013 standard provides a recognized framework for an ISMS and Tobruk’s consultants are qualified as Lead Auditors in its application.

A control audit and assurance is essential for organisations who want confidence that their data, systems and people are protected. Our information systems auditors are highly experienced and follow international audit standards such as SSAE16 standard.

The additional steps post testing would be the following

Our Control Audit and Assurance Approach:

1. An initial engagement to scope the Audit
2. A meeting to agree the audit agenda
3. Pre-audit data collection
4. Onsite audit interviews
5. Preliminary finding
6. Draft report
7. Incorporate feedback from draft report
8. Final report
9. Briefing to management

Stage 1

## Vulnerability Testing

The Tobruk Security vulnerability testing and assessment process consists of the following broad stages:

1. Scoping and planning
   1. Defining the target
      1. IP Addresses
      2. Test or production system
   2. Defining the threat scenarios
      1. External – Generic Internet threat
      2. External – Moderate Internet threat
      3. External – Sophisticated threat using Internet
2. Information provision

The information provision involves conducting a number of Internet related searches on common forums, Internet search engines and IP/domain searches. This aids in gathering possible threats and access points that may be publically accessible.

Information about the technical design of the target system allows the tester to either simulate a sophisticated attacker who might obtain insider information. It also allows a more efficient testing approach, focussing on areas where there are known vulnerabilities

1. Discovery

The discovery phase is used to determine what information can be identified about an organisation’s infrastructure through conducting passive network surveillance across the organisation’s infrastructure. This testing can include network surveying, port scanning, system identification and application identification.

1. Enumeration

The Enumeration phase is focussed on confirming the hosts and services identified in the Discovery phase and identifying further information about the hosts and services.

Further information will include the operating systems of hosts, patch levels and applications running etc.

This information is critical in moving to the next phase of Vulnerability Mapping which will seek to identify and confirm the existence of any vulnerabilities associated with the hosts and services.

1. Vulnerability mapping

Based on the Discovery and Enumeration phases any potential vulnerabilities are identified with the available services. Vulnerabilities are based on the specific services identified during the Discovery and Enumeration phases.

Vulnerability research and verification also ensures that the exploits and vulnerabilities identified do actually exist and are not false positives. An assessment of the difficulty of exploiting the vulnerability will also be made at this phase.

1. Exploitation

Note that exploitation is out of scope for this engagement. During the Exploitation phase the vulnerabilities identified during the previous phases are attempted to be exploited.

Tobruk will provide ongoing consultation with the client throughout this phase to determine the level of exploitation that may be provided. For example, there are some exploits that may not be appropriate to undertake.

Denial of Service exploits will not be undertaken unless explicitly requests and authorised by the client.

1. Present results and validate findings with client

Tobruk will communicate on an ongoing basis throughout the testing process. This is especially important where security issues are identified that may require immediate remediation prior to delivery of a final report.

At the completion of formal testing Tobruk will meet with the client and discuss the findings from the testing and discuss and final report requirements.

1. Deliver report

At completion of the testing and consultation Tobruk will provide final reporting in accordance with client requirements.