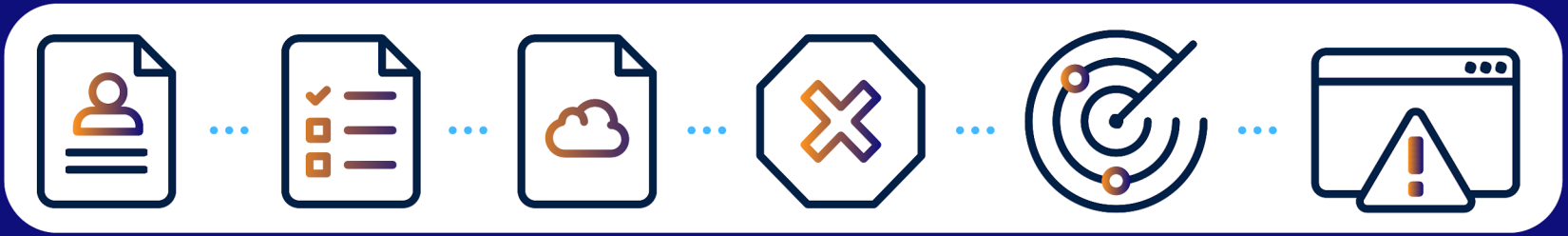
Elmdale
IT Services
Ltd

Security Posture Review

elmdaleit.co.uk

Elmdale Security Posture Review

An effective security posture should incorporate people, process and technology and cover incident prevention, detection and response.



Prevention based strategies alone are no longer adequate, the focus should now be on cyber resilience. **91%** of business leaders recently surveyed responded that cyber security was important to their business. Yet only **57%** said they had a formal cyber/information security strategy.

The Elmdale Security Posture Review is a detailed assessment of your full security posture, covering policy, processes and technology platforms.

Our consultants review the critical areas for remediation and practises and then map them against industry leading practice.

From this we create a maturity score of your security posture, identify risks and areas for remediation and provide you with guidance around the high priority issues identified and the steps recommended to remediate them.

Security Posture Review

Our Methodology

Our starting point is to understand your business in detail and your desired outcome from the engagement. We assess your security posture against the National Cyber Security Centre's 10 Steps to Cyber Security framework.

In overview the framework covers the following topics:

1. Risk Management
2. Engagement and Training
3. Asset Management
4. Architecture and Configuration
5. Vulnerability Management
6. Identity and Access Management
7. Data Security
8. Logging and Monitoring
9. Incident Management
10. Supply Chain Security

The initial phase

During the initial phase of the service we talk you through the framework and thereafter assess the maturity of your security posture against it.

Your maturity level is assessed by reference to our Capability Maturity Model, which aligns to the CMMI and ITIL maturity models.

The maturity levels are as follows:

0. Non-existent
Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.

---

1. Initial/Ad Hoc
There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.

2. Repeatable but Intuitive

Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

3. Defined Process

Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

4. Managed and Measurable

Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5. Optimised

Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

Security Posture Review

How we do it

The audit is delivered by gathering information in a variety of manners; initially via detailed questions provided to key stakeholders, follow-up interviews with these stakeholders, follow-up interviews with these stakeholders to discuss their responses and finally review of any pertinent documentation.

A typical engagement includes:

Pre-engagement questionnaire

This is to help us to understand your current systems, controls and environment. This information provides the consultant with the awareness of your environment and ensure he/she is as equipped as possible before the engagement begins.

Document Review

We review your current policies and procedures ahead of the stakeholder interviews. This will allow us to understand your current policies and procedures maturity, then test effectiveness.

Stakeholder Interviews

We conduct 1-to-1 interviews (maximum of 8). This can be carried out remotely and should include representatives from across the IT organisation, as well as senior business managers and HR.

Interviews are recorded, with the participant's permission, which allows us to go back through the recordings to confirm our notes, rather than having to disturb your stakeholders unnecessarily with clarification queries. Sometimes we will need to confirm or qualify certain points and in these circumstances, we will arrange a follow up conversation or meeting.

Some interviews may involve more than one stakeholder at the same time, depending on the nature of your organisation and how responsibilities are allocated. It is important that full transparency is provided to our consultants during the interview process.

During the interviews we use our security posture assessment tool to build a comprehensive profile of your security architecture, processes, technologies and more. We then map this profile against the Capability Maturity Model to provide an objective assessment of your current security posture.

The assessment tool has been put together by reference to leading security standards and management systems as well as our own personal experience. It is constantly reviewed and refined.

What you get

We provide you with a written report setting out our findings, but focusing more on our recommendations.

The report will score your security posture methodology by reference to our Capability Maturity Methodology and the steps you should take to improve your posture. High impact risks will be prioritised for immediate remediation.

We complete the engagement by presenting our findings and recommendations to you and discussing next steps.

Safeguard your digital frontier with confidence.

Security Posture Review

Drop us an email or give us a call with any questions or to find out more.

sales@elmdaleit.co.uk

0118 982 1444

Elmdale
IT Services
Ltd

Leading The Way In Digital Business Solutions

Contact Us

sales@elmdaleit.co.uk
0118 982 1444