DSPT Healthcheck

A RICOH Company

All healthcare organisations in England that have access to NHS patient data and systems must measure and publish their performance against the National Data Guardian's ten security standards. Organisations are required to pass the Data Security and Protection Toolkit (DSPT) test to provide assurance they are practising good data security and that personal information is handled correctly.

The DSPT is also used by a growing number of healthcare organisations in Scotland, Wales, and Northern Ireland, as well as by some private sector organisations that provide services to the NHS.

Our DSPT Healthcheck is designed to help NHS organisations assess themselves against the technical measures required to pass DSPT.

The Service

Our DSPT IT Health Check assesses core infrastructure requirements covered within a dedicated IT security review and is designed to provide data to formulate answers to DSPT questions relating to technical measures. If required, the Secure Email Standard assessment (checking compliance to DB1596) can be included within scope.

Experienced MTI consultants will assess your existing infrastructure to help you understand the current standing of technologies and systems relating to DSPT assertion requirements.

Stage 1

What we test:

External network

External network penetration testing: To determine the flaws and risks exposed through your Internet Gateway we conduct a manual penetration test to provide a complete picture of all Internet-facing systems. To provide a high quality of service, we combine two methods of a tools-based vulnerability scan and a bespoke manual test to ensure all identified issues are fully investigated and false positives are eliminated.

Unauthenticated web application assessment: We conduct an unauthenticated scan of internet-facing web applications to determine adherence to the relevant DSPT assertion. A fully automated web application scan of the application will test for common misconfigurations or weaknesses that could lead to compromise of the application, the host server, or the underlying infrastructure.

Stage 2

What we test:

Internal network

- Internal network penetration testing
- Domain compromise assessment
- Operating system hardening build review
- Password reviews
- Anti-malware client review
- Wireless infrastructure assessment
- Networking equipment default password check
- Automated firewall configuration review VPN review
- Mobile device reviews

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation

Stage 3
Reporting

The formal report on testing phases will include the Security Assessment's objective, scope, executive summary of findings, risk grading, CVSS scoring, vulnerability description, recommendations, and contact details for the customer and test team, as well as CHECK/CREST/Cyber Scheme consultants' certifications.

Vulnerability register: To aid with remediation and compliance tracking, MTI will provide an Excel-based Vulnerability Register listing all issues found during manual testing, along with the CVSS scores in a sortable and editable format. Due to the volume of issues usually found, this does not include issues discovered during automated testing.

Deliverables

The health check service provides:

· A formal report detailing all issues found, identifying the severity and exploitability of each condition with severity ratings based on CVSS scoring.

· An action plan that sets out the recommended remediation steps and details the stages that help you track your remediation progress.

· Summaries of the business and technical risk that make the results accessible to all stakeholders.

· An outline of your path to a more secure environment.

Outcomes & Benefits

The health check delivers the following outcomes:

· Provides a thorough examination and test of the external, internal and cloud-based infrastructure.

· Details issues that comprise a threat to the integrity of the IT infrastructure and a barrier to DSPT compliance.

· Provides data to formulate answers to DSPT questions relating to technical measures.

· Outlines where elements of the IT infrastructure are configured correctly and securely.

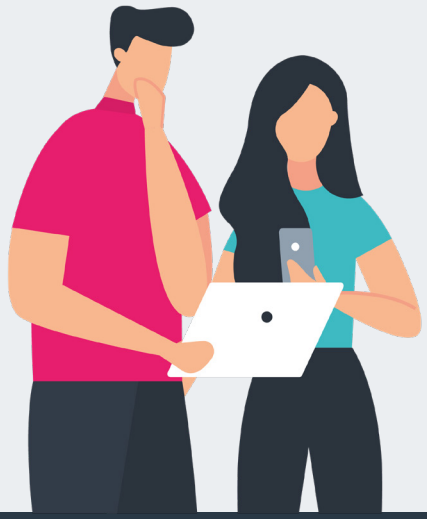
· Provides peace of mind by discovering vulnerabilities and outlining how they can be addressed.

Why MTI?

A longstanding member of global cyber security bodies, CREST and CHECK, MTI has been conducting penetration testing on IT infrastructure for more than 20 years. As one of the first companies to provide this service, we have developed a wealth of knowledge and skills in the tactics used by malicious users to gain access to corporate networks. This enables us to identify risks to your organisation and outline remediation measures to counter those risks.

MTI has supplied penetration testing services to local and central government, Critical National Infrastructure within the NHS and utilities sectors, the Ministry of Defence, the private sector and companies affiliated with the US Department of Defense.

The DSPT IT Health Check is a purely technical test but MTI can also assist with other elements of the review, such as Information Governance, Policies and Procedures and Staff Training.



Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation