D2NA™

TRANSFORM | PROTECT | SUPPORT

IT & Cyber Security Audit

What is it?

Our IT & Cyber Security Audit provides you with a robust overview of your current IT environment from a practical and security perspective.

Why do you need it?

The purpose of the IT & Cyber Security Audit is to identify and highlight key areas where changes are needed to improve business efficiency, the security posture of your IT network and protect sensitive data from an internal and external perspective. It gives you a strategic view of how to harness technology with a roadmap for the future.

What is involved?

On the next page is an outline of all the areas our IT & Cyber Security experts will investigate as part of the checks of your IT infrastructure. After performing these investigations, a report of their findings will be created detailing issues found. The report will also offer remediation advice to be followed internally or outsourced.

SEE NEXT PAGE FOR DETAILS OF THE D2NA IT & CYBER SECURITY AUDIT

CREST | VA | PEN TEST · IASME CONSORTIUM · CYBER ESSENTIALS CERTIFIED PLUS · ISO 27001 · Gold Microsoft Partner · aws partner network

Infrastructure Assessment

> **Network - WAN**
The engineer will inspect the firewall/router configuration and identify the type of internet connectivity the business is using, including how external sites are connected. An internet speed test is also performed to determine the ISP and bandwidth of the connection.

> **Network - LAN**
The make, model and configuration of all network switches is documented, where possible, to determine the topology and functionality of the internal network.

> **Network - Wireless**
Analysis of the wireless network configuration, connectivity and security is performed.

> **Applications**
The engineer will inspect all servers and document all server-based applications and their version numbers. The engineer will also document and discuss all business applications used by members of staff with the site contact and key people in the various departments.

> **Email**
Inspection of current email system (usually MS Exchange or Office 365), version and build numbers documented for any on-premise email systems. DNS settings are reviewed (SPF, DMARC, DKIM).

> **Backup/Replication**
The engineer will review how servers and data are backed up by the backup solution(s), including backup media, storage locations and security.

> **Physical Servers**
The engineer will physically inspect all servers and document their OS version, AV, role/function, make, model and serial number. A warranty check is then performed to confirm if the server has a manufacturer's warranty.

> **Remote Access**
The engineer will determine how users remotely connect to the network and how access is managed.

> **Virtual Servers**
The hypervisor make, model and basic configuration will be documented and all virtual servers inspected for OS version, AV, roles/functionality, applications and configuration.

> **Storage**
All SAN, NAS and removable storage is inspected and make, model, version, serial numbers documented. Manufacturer warranties are then checked.

> **UPS/Power**
All UPS units are inspected for load and runtime.

> **Domain Hosting**
Website hosting is reviewed and all available DNS configurations are documented for analysis by the engineer.

> **Endpoints**
Make, model, OS version and AV are documented for all PC's, laptops, tablets and mobile devices, where possible, for analysis by the engineer.

Cyber Security Assessment

> **Network Security**
A general overview of the entire network is gathered by investigating how devices are connected physically or wirelessly, and how geographical locations communicate (e.g. MPLS, VPN).

> **Patching**
The engineer will use different methods to determine operating system and firmware versions of network connected devices, internal device update schedules, and update management including mobile devices.

> **Password Policy & Management**
Internal password policies will be inspected and compared to actual users to identify user compliance. Systems for the management of passwords are checked.

> **Active Directory & User Access Control**
Active Directory users and groups are checked for anomalies and security best practises. Group Policies relating to password policy and workstation security are tested.

> **File Security**
File storage processes and solutions are checked for efficiency and security. Backup and redundancy processes are investigated.

> **Application Control & Sandboxing**
Application whitelisting for endpoints and mobiles (where applicable) are checked. COPE (company owned personally enabled) and COBO (company owned business only) devices are tested for restrictions. Anti-virus solutions are investigated for updates, scan schedules, and effectiveness.

> **Email Filtering**
Email protection is checked for availability and effectiveness by sending test files. Rules are inspected.

> **Web Content Filtering**
Web content filtering is checked for availability and effective by visiting test websites.

> **IT Security Policies & Processes**
The distribution and contents of policies are inspected for GDPR compliance as recommended by the ICO.

> **Physical Security**
Doors, windows, CCTV, access control, etc are checked for obvious weaknesses and best practises.

D2NA™

TRANSFORM | PROTECT | SUPPORT

CONTACT US TODAY TO BOOK IN YOUR IT & CYBER SECURITY AUDIT

E sales@d2na.com | T 0330 159 5969

CREST | VA | PEN TEST

IASME CONSORTIUM

CYBER ESSENTIALS CERTIFIED PLUS

ISO 27001

Gold Microsoft Partner

Microsoft

aws partner network