# Cyber Security Audit

CARETOWER
I·T· Security Specialists

# Cyber Security Audit

## A Cyber Security Audit Overview

As a business, security is one of the most important factors that keep you safe and running especially with the multitude of potential threats you might be facing. Cyber security audits are designed to be a comprehensive review and assessment of your IT infrastructure and your security posture. It can assist identifying threats, weaknesses, advise on best practice, make best use of your current solutions and so on.

Regulations such as the **GDPR** (**General Data Protection Regulation**) can impose hefty penalties in the event of a breach that results in exploited data. This is where a cyber security audit can help mitigate the consequences of a breach and show that you have taken the necessary steps to protect client and company data.

**Caretower can advise you on the best way to improve your cyber resilience. We can ensure your data is safe and protect your business/environment across multiple areas.**

## Caretower Offer Two Levels of Audit:

1

### Mid Level Security Audit

Full vulnerability scans, firewall regulation, Active Directory reviews and privileged account management.

2

### In-Depth Security Audit

Further adds on to the mid level with Network/Infrastructure Management, Policy Reviews, Monitoring & Risk and software/ hardware management.

## Mid Level Security Audit

Caretower offer two levels of audit – but each can be tailored to your environment and particular areas of concern and our specialist will discuss these requirements with you and put together a full scope of works. Our **Mid Level Security Audit** can provide you with:

- **Firewall Management** - Checks, which include firmware and rules, making sure they are being managed to regulatory compliance.
- **CAF Compliance** - Working within the CAF framework to deliver best practice/industry standards.
- **Full Vulnerability Scans** - In order to identify existing and potential failures/issues and remediate them.
- **Active Directory Configurations Review**- Using established practices for Group policies, software installation & management of removable media and necessary user accounts (including privileged account management & administrative access to create/delete users.
- **Full Governance Review** - With a deep dive into policies and procedures, a review of change control and checks for privileged access & 3rd party access.

# Cyber Security Audit

## In-Depth Security Audit

Our **In-Depth Security Audit** includes everything in the **Mid Level Security Audit**, but also:

- **Operational Review of Information** - Software and hardware assets management specifically relating to:
  - Registers for physical devices, software & data compliance.
  - Information, software & hardware asset tracking.
  - Management & deployment of applicable backup solutions, DR and business continuity.
  - Software & hardware lifecycle/deprecation management.
  - Endpoint protection and internet security provisions.

- **Monitoring & Risk** - A review which addresses aspect of monitoring & reporting with recommendations on log retentions, as well as regular reviews on:
  - Incident response management.
  - Table top planning, cyber security & technical training provisions.
  - Management of risk and what constitutes an acceptable risk.

- **Network/Infrastructure Management** - Policies & Procedures documentations, patch management (including 3rd party software & firmware perimeter), wireless device management and PCI compliance.

- **Policy & Procedures Review** - Based upon current regulatory expectations as well as the best practices. This will include but isn't limited to:
  - HR staff handbook and the relationship to operational policies and procedures.
  - IT Operations & employee guides.
  - Governance to the General Data Protection Regulation 2016/679 and the Data Protection Act 2018.
  - Onboarding of staff/employees and due diligence of suppliers.

- **Other Applicable Policies/Procedures Addressed** - Includes Security Responsibilities, Business Continuity & Disaster Recovery Plans, Protecting Assets & Information, Use of the Internet, Preventing Disclosure of Sensitive Information, Defence Against Virus & Malicious Software and more.

Call your Dedicated Account Manager to find out more about our services!

**0208 372 1000**

CARETOWER
I·T· Security Specialists