Cyber Security Audit

TiG Data Intelligence

Cyber Security Audit

Recommended checklist for conducting a cyber-security audit within a business

TiG Data Intelligence

Introduction

What is a Cyber Security Audit and how can it help your organisation?

A cyber security audit is designed to be a comprehensive review and analysis of your business's IT infrastructure. It identifies threats and vulnerabilities, exposing weaknesses and high-risk practices.

Regulations such as the GDPR (General Data Protection Regulation) can impose hefty penalties in the event of a breach that results in exploited data. A cyber security audit will help mitigate the consequences of a breach and demonstrate that your organisation has taken the necessary steps to protect client and company data. Our cyber security specialists can advise on the best course of action to vastly improve your cyber resilience, securing your data and protecting your business.

Who is the cyber security audit designed for?

Cyber security audits are a valuable tool for organisations that haven't yet documented their internal and external risks, vulnerabilities and threat exposure. It is also applicable to businesses that have expanded, implementing various software and security controls but are inevitably overwhelmed by the volume of data being processed in daily communications.

The audit is designed to check the cyber security measures in place and prompt further thought about target areas businesses can focus on to improve their cyber security.

The audit

Information Security Governance and Risk Management

A review of available policy documents.

- ☐ What is the status of the organisations security policies?
- ☐ Do the security policies demonstrate linkage to the business objectives?
- ☐ Is there budget allocated for the purposes of information security risk management?

Identity and Access Management

A review of the recruitment / provisioning of new users.

- ☐ Do the recruitment processes include reasonable provision for security?
- ☐ Is personally identifiable information held securely?
- ☐ Is the principle of least access implemented?

- ☐ Is there reasonable separation of services?
- ☐ Does the organisation have robust processes for good / bad leavers?

Disaster recovery / business continuity preparedness

A review of the ability of the organisation to recover from an IT disaster event.

- ☐ Is the DR plan complete?
- ☐ Has it been tested and what were the outcomes?
- ☐ Does the organisation have sufficient redundant components to avoid common disaster scenarios?
- ☐ Is the Business Continuity plan complete?
- ☐ Has it been tested and what were the outcomes?

Security Incident response

A review of the ability to minimise the impact from a security event.

- ☐ What is the process for remediation of a security event?
- ☐ Does the organisation have service improvement processes?

Technical risk avoidance

Does the organisation have reasonable preventative measures in place?

- ☐ What is the approach to encryption?
- ☐ Are critical information assets exposed to risk?
- ☐ Are information assets categorised efficiently?
- ☐ Is remote working secure?
- ☐ Is the location of at rest data appropriate?
- ☐ Are staff sufficiently well-educated?

About TiG

We work in partnership with our clients to deploy the right technology, with provable security measures, full compliance and simplified due diligence reporting.

Our team includes industry compliance experts and analysts whose role it is to securely manage every project and managed service we work on.

We are proud to hold the following security accreditations:

Contact us:
t: +44 (0)20 7100 3310
e: info@tig.co.uk
www.tig.co.uk

TiG Data Intelligence

With us, it's personal