COGNISYS

COMPLIANCE

Cyber security review

Let us help you identify and recognise risk across your organisation's people, processes and technology.

A comprehensive audit can help you to check that your information security controls are operational and effective, and build a roadmap for improvements to strengthen your security posture.

Undertaking a review will provide your organisation with an independent third-party assessment of your current state and our experts are there to help you develop a strategy to increased maturity in the future.

Overview

The following areas are included within the assessment:

- Security controls.
- Key cyber assets.
- Business continuity.
- Responsibilities and roles.
- Incident management.
- Staff awareness and current training.
- Risk register.
- Policies.
- Cyber risk governance.
- Any contractual, legal or regulatory obligations.

The technical areas

- How you monitor security.
- Your access controls.
- Perimeter controls – firewalls, IDS, IPS Proxy.
- What anti-malware is in place.
- An overview of user privileges.
- We review IT core infrastructure devices and sample endpoints.
- Data classification.
- Mobile Device Management (MDM), Multi-Factor Authenticator (MFA), and mobile working.

The physical areas

- How safe your perimeter is.
- Designated secure areas.
- The physical security of your IT systems.
- Any 3rd party access or policies.

Why have a Cyber Security Review?

Our cyber reviews give you a 360 degree view of your current state, providing objective guidance on the risk inherent in your business.

Reviews are non-intrusive, meaning that the day-today running of the business can continue, while we interview and discuss various areas of security with your team.

Creating a security baseline and targets for improvement means you have an actionable plan which can then be tracked and measured to provide you with attainable goals for improved maturity.

Report

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BACK TO CONTENTS