

Cybersecurity maturity assessment



Overview

Many events can prompt your organisation to put a spotlight on cyber security. Perhaps there have been high profile security incidents in your sector, or even in your organisation itself?

You might be planning to undertake a digital transformation programme or introduce new systems and technologies; or there might be new cyber security regulations on the horizon that you need to be prepared for.

Irrespective of your drivers, a maturity assessment is the ideal starting point to establish a baseline which provides visibility of where you are and what you need to do to improve.

While it can take time to implement programmes of change across the whole organisation, our cyber security maturity assessment enables managers to set a benchmark against industry standards, highlight areas for improvement, measure progress and provide a visual way to communicate progress to their leadership.

Our approach

Our proprietary framework, which is used and trusted by Capita's largest clients in both the public and private sector is a 1-week engagement where we:



Discover

- Understand the business goals and objectives
- Collect policies, standards, and procedures
- Understand employee culture and training,
- Fact finding consultations with small number of stakeholders focusing primarily on:
 - Information security governance
 - Cyber risk management
 - Information security / cyber programme development and management
 - Information security incident management policies and procedures



Markets / Industries

- All markets and industries



Analyse

- Assess documentation and processes
- Clarify understanding with key stakeholders
- Review existing security control



Report

- Deliver report and findings outlining key issues that may require further discussion or remediation.
- Provide a high-level remediation plan

For more information please contact:



Jim Fox CISM, MBCS, MSyl
James.fox2@capita.com

capita