secarma
CYBERSECURITY EXPERTS

A Advise C Certify T Test

Cyber Security Maturity Assessment (CSMA)

Our Cyber Security Maturity Assessment takes a holistic view of your organisation's current security program looking beyond technical configuration, in relation to its ability to protect, detect and respond to security threats.

Secarma has developed a simplified version of the NCSC Cyber Assessment Framework, tailoring the assessment to focus on responsive solutions organisations can implement to become more robust.

Who Is It For?

All businesses, regardless of size should be given the opportunity to develop a thorough understanding of the risks they face and be given direction by a trusted advisor to improve their own cyber security maturity.

This assessment is ideal for organisations starting on their security journey right through to those CISOs and IT managers who are struggling to get Board buy-in to security projects.

It's also a valuable tool for businesses who may have some technical security skill but no wider governance structures, or companies that have recently formed, acquired or been devolved.

How Can We Help?

Many organisations have the intention to improve their cyber security, but simply don't know where to start or worry they may miss an area of concern. Secarma's CSMA mission is to simplify implementations that align cyber security practices with your organisational objectives and policies.

We will perform a review on your current security posture through an initial orientation meeting, a documentation review and interview workshops. This will give your organisation a deeper understanding, not only in the areas of security strategy you are carrying out successfully but to what degree of maturity has been achieved, and how to improve it.

What We Test

Our CSMA evaluates an organisation's preparedness and grades their maturity in the following areas:

- **Risk Management**
  Security policies ranging from organisational roles, security training, assessing risks and communicating security goals.
- **Security Protections**
  Documenting and grading an organisation's technical enforcement of security policy.
- **Incident Detection**
  Monitoring the essential services for security concerns which may impact the security of the systems and the effectiveness of security measures.
- **Minimising Impact** - An organisations ability to address incidents that are detected in terms of planning, testing, and backing up vital information.

3 Archway, Birley Fields, Manchester M15 5QJ
0161 513 0960
secarma.com
actnow@secarma.com

Interaction with your organisation is a must to complete the CSMA. Our experts will be reviewing policy and playbooks against best practice, interviewing staff to ensure that policies are well communicated and enacted and delving into each maturity area to assess the following points:

Risk Management

- Security Policy
- Board-led Security Culture
- Security Awareness Training
- Supply Chain
- Asset Management
- Risk Management
- Security skills & responsibilities

Security Protection

- Access Control
- Secure Configuration
- Penetration Testing & Vulnerability Management
- Data Management
- Network Segmentation

Incident Detection

- Monitoring and Alerting
- Threat Intelligence
- Staff Capability
- Incident Management & Escalation

Minimising Impact

- Response Planning
- Response Testing
- Backups & Recovery Capability

Results

Post assessment the organisation will receive a report of findings using an objective scoring methodology to assess each area of the CAF framework. This comes complete with an executive summary and a series of short and long term objectives that offer a real world insight into the areas in which the organisation may improve.

Depending on your organisations goals, the CSMA report can reference standards that you are working towards and map to the relevant controls such as ISO27001 or Cyber Essentials.

3 Archway, Birley Fields, Manchester M15 5QJ
0161 513 0960
secarma.com
actnow@secarma.com