Cyber Security Maturity Assessment

CGI's Cyber Security Maturity Assessment (CSMA) highlights potential organisational issues, technical vulnerabilities and compliance gaps. This enables organisations to manage these vulnerabilities, close the gaps and reduce risk very quickly.

Why you need to take action

Threats from all quarters are growing in complexity and volume, whilst the security-related legislative and regulatory burden is increasing. These new standards and regulations mean many organisations now require that their partners and suppliers demonstrate that they have taken appropriate steps. GDPR in particular has introduced large financial penalties for not applying appropriate protection to safeguard your and your customers' personal data.

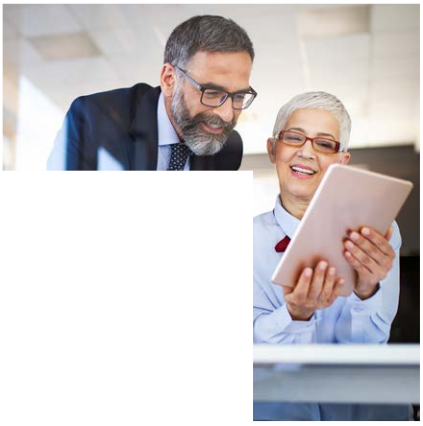
There is an increasing need for organisations to assess the maturity and effectiveness of their cyber security. This is driven by the significant impact of failing to understand and address risks. However, many risk-related approaches encourage 'box-ticking' without addressing reality. Managing the threat landscape successfully requires an agile response to constant, rapid change, whilst maintaining a solid, pragmatic cyber security regime. Establishing how an organisation meets these threats is best done by assessing maturity in respect to that regime. CGI's CSMA methodology provides an established and methodical means to do so.

Our approach

CGI Cyber Security runs Risk Management 'as a service' and uses CSMA as one of the means to support this approach. CSMA focuses on critical systems and controls. It is based on the well-established UK Government Information Assurance Maturity Model (IAMM) but has been highly evolved to make it appropriate for use in any environment or sector.

CSMA covers 6 'domains':

- Leadership & Governance
- Information Risk Management
- Education, Training and Awareness
- Assured Information Sharing
- Through Life Information Assurance
- Compliance



Benefits

- Increase employee engagement and encourage your people to take security seriously with our collaborative approach.
- Reduce the frequency and impact of security breaches and incidents thanks to a greater understanding of vulnerabilities.
- Gain a clear overview of how maturity is improving thanks to straightforward graphics and reporting.
- Ensure strong compliance and alignment with a range of common standards.

The process seeks to understand how mature an organisation is against these 6 domains by establishing its position against the following statements:

Leadership & Governance

- Information Security Policy and Strategy is current, proven and endorsed by the Main Board.
- The Main Board champions Information Security across the organisation, through its own behaviours.

Education, Training and Awareness

- A targeted Information Security Education, Training and Awareness Programme addresses current threats and includes annual re-examination.
- Security Education and Training supports effective security culture change.

Information Risk Management

- nformation security risks are regularly agreed, reviewed, recorded and are visible to the Main Board.
- Operationally critical information assets and associated systems are identified and commonly understood.

Through Life Information Assurance

- The Main Board has confidence in the current status of the controls protecting systems and/or services and are aware of the improvements needed.
- The Main Board is confident that security incidents will be identified and managed effectively.

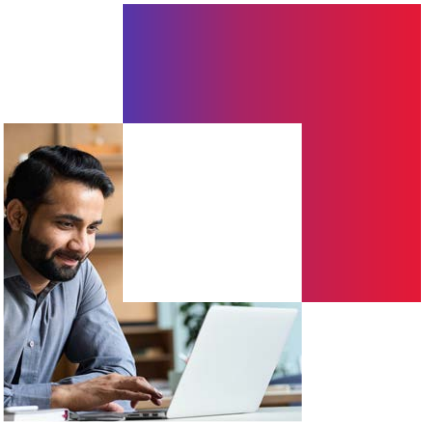
Assured Information Sharing

- There is an effective process for sharing information securely that encompasses business partners and other third parties.
- The Main Board has confidence in the security of connections with third parties.

Compliance

- The Main Board is confident that they understand the compliance obligations placed by others and ourselves to meet business objectives.
- There is an effective compliance assurance regime that ultimately feeds into an actively-engaged Audit Committee.

The CSMA process is evidence-based, providing a rapid, high-level indication of information security maturity. It delivers initial guidance on the direction of a more detailed analysis. To this end, CSMA is allied to the CGI proprietary IRIS Risk Assessment, Security Culture Assessment and accredited Penetration Testing tools and methodologies. CSMA can be used alongside the Acuity RM STREAM-based Risk Management as a Service offering. CSMA provides natural direction and a 'lead in' to other potential services, including Security Engineering, Advanced Threat Intelligence (ATI) and Security Management as a Service.



About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industry sectors in 400 locations worldwide, our 77,000 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit cgi.com/uk/cyber-security
Email us at cyber.enquiry.uk@cgi.com