Cyber Compliance Assessment

SA Group's comprehensive Cyber Compliance Assessment service is designed to give you objective intelligence around your compliance to a specific standard of your choice. This understanding is critical especially if you're embarking on a certification path, or working on a tender where your client wants evidence of compliance without the requirement of certification.

A Cyber Compliance Assessment gives you evidence of compliance where you meet the standard, and remediation plans to bridge any gaps. Benefits for your organisation include:

INSIGHT: Gain useful intelligence into threat sources, vulnerabilities and potential impact.

IDENTIFY GAPS: Uncover how vulnerable your data is to Cyber attack.

ARTICULATE CYBER SECURITY: Have the right information to be able to articulate security to key stakeholders.

MITIGATE RISK: Be able to take appropriate action to minimise the likelihood or impact of a cyber event.

EVALUATE YOUR ESTATE: Gain valuable intelligence into effective cyber security and baseline your posture.

SA GROUP
CYBER | P3M | TECHNICAL

Standards we cover include:

NIST CSF: Created by the National Institute of Standards and Technology, the framework covers the requirements to Identify, Protect, Detect, Respond and Recover from a Cyber attack.

ISO 27001: This is an international standard on how to manage security. It aids organisations on the creation of an Information Security Management System (ISMS).

FFIEC: The Federal Financial Institutions Examination Council is a body that regulates the security requirements within the banking sector.

10 Steps to Cyber: Devised by the UK's National Cyber Security Centre (NCSC), the 10 Steps to Cyber sets out the minimum Cyber requirements any organisation should be implementing.

Cyber Essentials: A UK Government-backed initiative to help organisations protect themselves against cyber attacks.

A comprehensive assessment model

Pre-assessment phase	· We will gain a full understanding of your requirements and conduct a scoping exercise with a cyber expert to ensure the assessment covers the areas you want.
Assessment phase	· You will be assigned a dedicated cyber specialist and we endeavour for this to be the same expert who conducted the scoping exercise. · The cyber expert will most likely require access to people, company policies, processes and technical configuration. As each assessment is slightly different, the level of information could change. · For the duration of the assessment the cyber expert will be available to you to discuss any aspect of it and, if required, the cyber expert can update you on a regular basis.
Report phase	· Once the assessment is completed you will receive a comprehensive report. · Every discovery within the report will be substantiated with evidence and recommendations for either fixing, increasing maturity or mitigating the risk, enabling you to make the most informed decision possible. · There will be a meeting after the report is issued to allow you to raise any further questions or clarify any aspect of the report.

SA Group's Cyber P3M Wrap™ Service Model

Our consultants blend P3M and Cyber expertise, encompassing a wider understanding of your organisation's needs and ensuring a more thorough, relevant delivery.

Why SA Group?

SA Group has been tested and appointed by Crown Commercial Services as a Supplier of Cyber Services to HM Government. We have a proven track record of delivering cyber assurance in the highest security environments, including the MoD and other government departments plus major blue chip commercial clients.

For more info:
E: cyber@sa-group.com
T: 03333 583340

SA-Group.com

SA GROUP
CYBER | P3M | TECHNICAL