CYBER MANAGEMENT ALLIANCE

ONE-DAY NIST CYBER HEALTH CHECK

Based on the US NIST Cybersecurity Framework & ISO 27001:2013

NIST

The One-Day Cyber Health Check, based on the NIST Cybersecurity Framework (NIST-CSF) is a fixed, low-cost assessment to determine your organisation's cybersecurity health and readiness to respond to cyber-attacks.

The health check covers five key pillars of cybersecurity, namely, Identify, Protect, Detect, Respond and Recover and is based on the US NIST CSF.

In this cybersecurity audit, we take a cursory look at the threats, vulnerabilities and risks your organisation faces and conduct a compact review of related materials including policies, processes and procedures

Our framework enables us to offer a standards-based approach that is flexible, repeatable, performance-based and cost-effective. The diagram below provides a breakdown for each of the five key pillars.

info@cm-alliance.com https://cm-alliance.com +44 203 189 1422 @cm_alliance

Benefits:

- Fixed, low-cost appraisal of your organisation's cybersecurity.
- Timed access to a highly qualified security consultant at a fixed cost.
- Likely opportunity for significant cost savings.
- Output and recommendations aligned against a well-understood, internationally-recognised framework (NIST CSF).
- An enhanced understanding of your organisation's strengths and weaknesses in incident response.
- Easy to understand recommendations to achieve tangible improvements.

Our approach:

We send you a link to a self-assessment questionnaire that you complete. After we receive payment, you are assigned an experienced cybersecurity consultant who will spend up to 4 hours with you on a single call.

The diagram on the right further describes the straightforward process to initiate and complete the One-Day Cyber Health Check.

What We Examine:

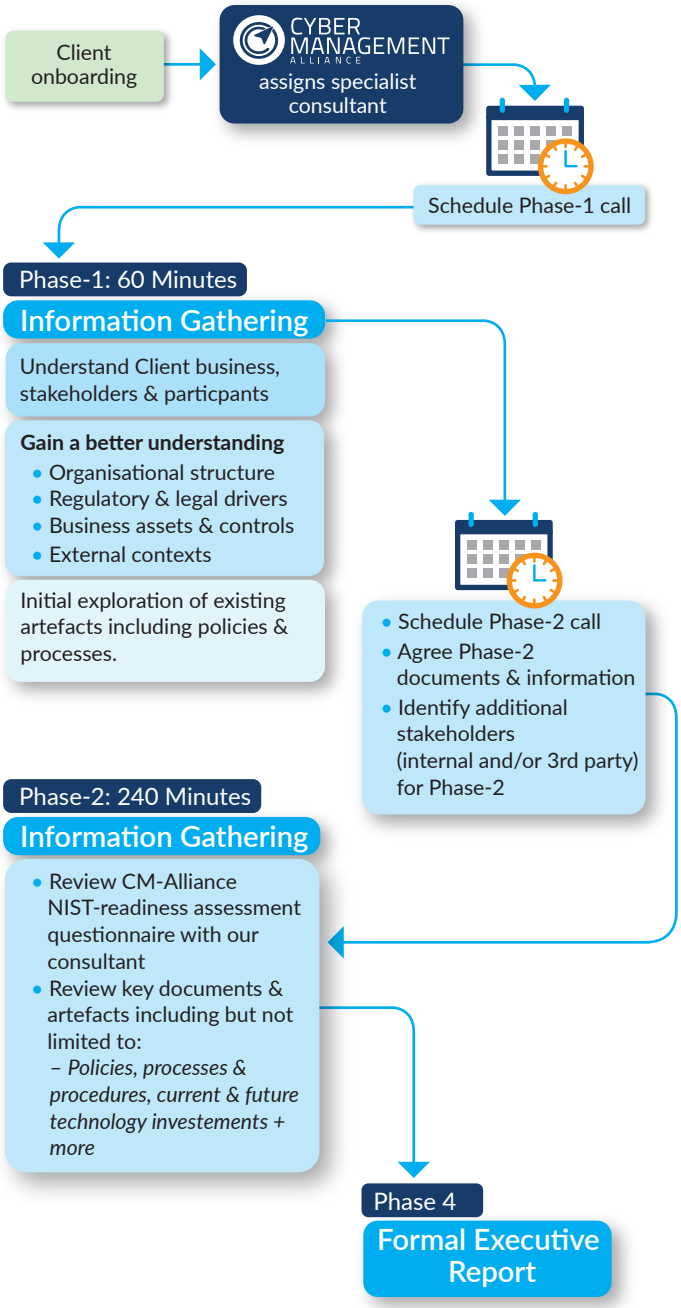
As part of our One-Day Cyber Health Check, we will need to see key document artefacts including, but not limited to cyber security related policies and processes, incident response processes, key strategy documents. Where possible, we will also want to speak to your key suppliers who may be providing your cybersecurity services.

Output:

We produce a concise report that highlights our key observations and opinions on your organisation's cybersecurity, compliance and overall incident response readiness, clearly highlighting any critical deficiencies that need urgent attention. This is mapped against the NIST cybersecurity framework. The report will include a summary list of recommendations.

Your Obligations:

For this exercise to be successful, you must have all your resources available and documents ready for the Phase 2 call (see image).



Please note: *This is a fixed, low-cost opportunity for you to highlight your strengths and weaknesses. We do not test any controls. We do not deep-dive into any processes and/or documentation. We will take your responses at face value and base our reports and recommendations on those responses.*

info@cm-alliance.com https://cm-alliance.com +44 203 189 1422 @cm_alliance