CYBER MANAGEMENT ALLIANCE

CYBER INCIDENT RESPONSE MATURITY ASSESSMENT

A mature, cyber-resilient organisation can be defined as a business that can continue to operate, service its clients, deliver a public service, satisfy its shareholders and continue to make a profit, despite being under a cyber-attack.

An effective, responsive and resilient organisation is always alert and on the look-out for early signs of malicious activity and pounces on the slightest of suspicious events with the intention of nipping them in the bud.

Summarised, a resilient business can:

- Rapidly detect and swiftly respond to an incident,
- Quickly and accurately identify, investigate and classify an incident,
- Safely recover from an attack and securely resume business operations.
- Capture, analyse and process data from the attack to create, share and maintain attack knowledge.
- Resume business operations with zero to little disruption.

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

Benefits:

This comprehensive, no-holds barred assessment, provides a 360-degree view of your organisation's cyber incident response and crisis readiness. We don't just interview stakeholders, we scrutinise each and every in-scope artefact and insist on supporting evidence for each item.

The Cyber Resilience Maturity Assessment is one of our most comprehensive, evidence-based assessments and it comes with an executive summary and detailed 'improvements' report. This audit also evaluates the SIEM and other technology stack implementation and the organisation's SOC operations.

- Obtain a comprehensive, 360-view of your organisation's cyber-resilience maturity measured against easy-to-understand NIST-based Incident Handling categories.
- Understand how your approach to incident response aligns with NIST's approach to incident response.
- Understand how your approach to incident response aligns with ISO 27001:2013's Annex A.16.1, Incident Management Lifecycle.
- Gain a deep understanding of your detection, response and recovery capabilities across the breadth and depth of your organisation's operations and strategy.
- Identify upgrade opportunities across a cross-section of your organisation's pillars of people, processes and technology.
- Identify improvements in operational workflows in the Security Operations.
- Significant opportunity to improve the whole organisation's cyber resilience posture.

What We Examine:

During our comprehensive wCyber Incident Response Maturity Assessment, we:

- Review documentation sets including policies, processes, procedures and technological standards.
- Review monitoring coverage, configured alerts, processes, use-cases and use-case-responses.
- Interview key stakeholders including senior management, management and technical resources.
- Will attempt to understand your monitoring landscape, SIEM and related detection and response technology.
- Review incident lifecycle management approach, processes and procedures.
- Review incident handling process, SOC team structure and skillset.
- Evaluate inter-departmental cooperation in incident handling.
- Review incident handling timelines against the defined processes.

Stakeholders:

One of the main objectives of this exercise is to collate and understand what the expected outcome of the service is. To this end, we seek to speak to stakeholders including, but not limited to:

- Project sponsors
- Executives including CISO, IT Director, IT Security
- Change / Service Management
- GRC team / risk team
- Head of Security Operations, Security Engineering, Forensics
- Third-party and supply chain involved in supporting the security service
- Security analysts operating the SIEM
- Threat management team, network security, AD team, Windows/Systems team

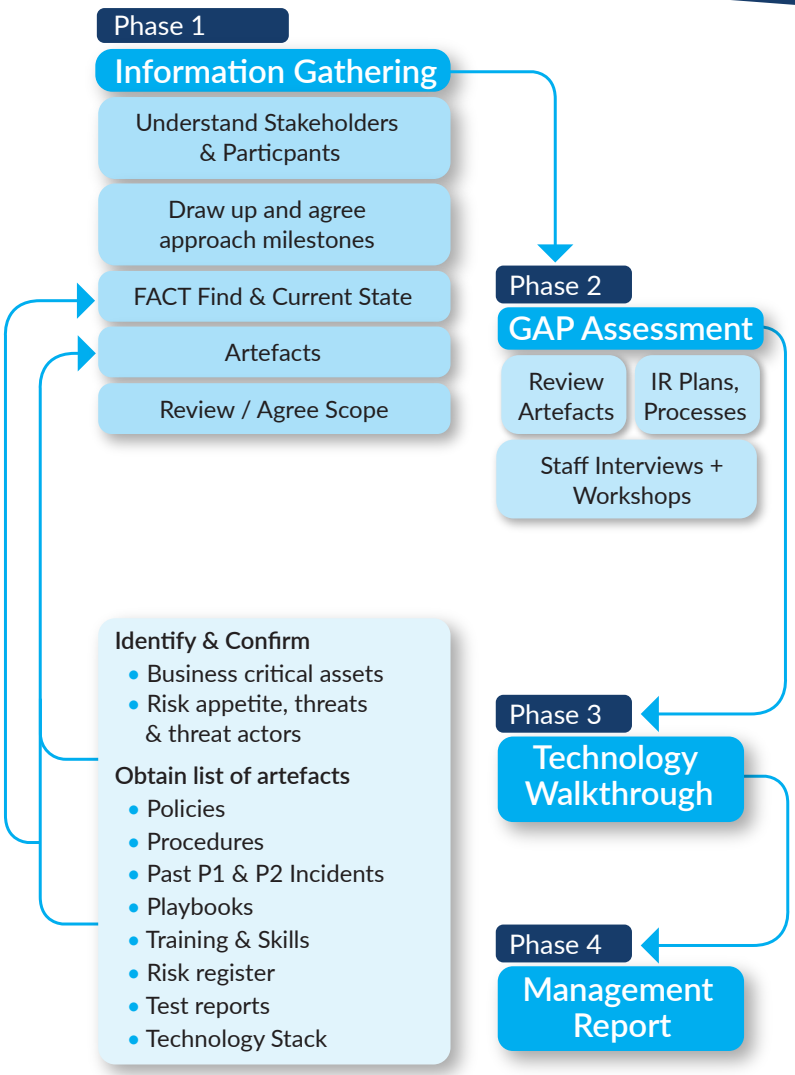
Approach:

We adopt the same rigour, discipline and evidence-based approach to all our assessments. In Phase 1, we are in a 'fact-finding' mode and want to read and consume all the necessary information.

Although we speak to staff in Phase 1, we tend to have more meaningful discussions in Phase 2, as we are more informed and hence more prepared with the right questions.

For the technology assessments, we prefer technology walkthroughs so we can get a feel of the setup, mode of use and configurations. We also get a feel of what a 'day' looks like for the operator of the technology.

We then complete the assignment with a management report.



Sample Breakdown of an Assessment Schedule:

Please note this is an approximation and the actual effort may vary depending on the client, the size of the SOC, the number of analysts and other factors.

Description	Total Duration
Initial meetings with Key stakeholders	10 hours
Multiple detailed meeting with Analysts	32 hours
Multiple meetings for SIEM/technology/ use-case walkthrough	24 hours
Meetings with security engineering	8 hours
Documentation review	32 hours
Initial meetings with other key departments	4 hours
Review, analyse and examine all inputs	16 hours
Report writing	16 hours
Total	**242 hours**

**Analysts = (SoC manager, IR team, threat intel team, Tier 1, Tier 2, Tier 3 analysts)*

Output:

You will receive a report with an executive summary accompanied by detailed findings, along with clear and easy-to-understand numbered recommendations. You will also receive a maturity score with an explanation of what it means and how to improve the score.