

Operational Capability Maturity Model

Govern & Assure

Embedding Cyber Security across your organisation

DEV/NUL



Enables executives to measure, benchmark, and mature the organisation's cybersecurity governance and operational capabilities — ensuring that cyber investments translate into effective risk management, regulatory assurance, and resilient business performance.

More detail

Our Cyber Security Govern & Assure — Operational Capability Maturity Model (CMM) provides a structured, evidence-based assessment of how effectively cybersecurity is embedded across your organisation. Using globally recognised frameworks such as NIST CSF, ISO 27001, CMMI, and COBIT, we evaluate your governance structures, operational processes, and cultural integration to determine current maturity and identify a clear path for improvement.

This service helps answer a critical question for executive leaders: "How mature, effective, and resilient is our cybersecurity programme — and what must we do next to strengthen it?"

Benefits

This service is particularly beneficial for organisations who want:

- An objective view of cybersecurity maturity across governance and operations.
- To ensure investment aligns with risk reduction and business goals.
- Confidence when facing regulatory scrutiny or audit requirements.
- A structured roadmap to guide capability development.
- Clear executive-level insight into strengths, weaknesses, and improvement priorities.

What's included in the Dev/Null service?



Governance & Operating Model Assessment:

An evaluation of your cybersecurity governance structures, roles, responsibilities, and decision-making maturity. This includes integration with enterprise risk management and alignment with business operations.



Capability Maturity Assessment:

A thorough review of maturity across key cybersecurity domains. This assessment benchmarks your organisation against global standards and identifies strengths, gaps, and opportunities across people, processes, and technology.



Risk & Compliance Alignment:

Analysis of how current capabilities support regulatory obligations, risk appetite, and audit expectations. This includes identifying control gaps and compliance risks across frameworks including NIST, ISO, CIS, and SOC 2.



Target Maturity Definition & Improvement Roadmap:

A structured roadmap outlining the steps required to achieve target maturity levels. This includes clear milestones, resource considerations, and prioritisation aligned with business outcomes.



Metrics, KPIs & Executive Reporting:

Development of meaningful metrics, KPIs, and KRLs to enable ongoing governance, performance measurement, and effective executive reporting. Dashboards and summaries support informed decision-making.



Continuous Improvement & Programme Evolution:

Support in establishing a governance cadence for ongoing reassessment and continuous improvement, ensuring the cybersecurity programme evolves with the threat landscape and organisational change.

Why Dev/Null?



Responsive:

We stay flexible and adapt to your priorities, whether that means shifting focus within a project or responding to an emerging threat to provide the best security for you. Our fast-turnaround, communication, and flexible engagement models keep you moving forward without delays.



Evolving:

Continuous learning is at the core of our culture: we routinely assess, refine, and re-engineer our processes, tools, and skills to stay ahead of the threat landscape. This mindset translates into more effective, efficient, and resilient solutions for you.



Sustainable:

We design security architectures and practices that endure, focusing on long-term resilience rather than quick fixes. By embedding best practices, automating controls, and aligning with your business roadmap, we foster a culture of continuous improvement.



Established:

Our team brings deep operational experience developed across a broad range of industries and security domains, backed by proven industry and vendor certifications, and a portfolio of real-world successes. That depth of knowledge lets us solve complex problems with confidence and speed.



Enabling:

Beyond delivering services, we actively coach your staff, sharing best practices, conducting workshops, and providing hands-on training to mature your capability. The result is an empowered internal team that can sustain and expand the gains we deliver.



Actionable:

Complex cybersecurity concepts are distilled into plain language, ensuring every stakeholder, from executives to engineers, understands the risks, options, and recommended actions. This clarity drives informed decisions and smooth collaboration across your organisation.

Choose Dev/Null

Selecting the right partner for a maturity assessment is essential. At Dev/Null, we combine deep operational expertise with established assessment methodologies to provide clarity and direction. Our team has extensive experience across security governance, risk management, operations, and assurance functions. We translate complex cyber challenges into actionable insights, helping executives make informed decisions that strengthen resilience and operational effectiveness.

Book a conversation with one of our consultants to explore how a CMM can protect you.

info@devnullsecurity.co.uk