Cyber Project Management Office

DEV/NULL

Design & Build

Disciplined, transparent, and outcomes-driven delivery

The Cyber Security landscape is always changing with new threats and vulnerabilities. Keeping pace with the changes using existing or new technology is essential to defending your organization. Our Cyber PMO service enables disciplined, transparent, and outcomes-driven delivery of cybersecurity initiatives that align with business objectives, regulatory requirements, and enterprise risk appetite.

More detail

Our Cyber Security Program Management Office (PMO) service provides the governance, structure, and oversight required to successfully plan, execute, and sustain cybersecurity programs at scale.
By integrating project management discipline with cybersecurity expertise, the Cyber PMO ensures that strategic initiatives deliver measurable risk reduction, operational improvement, and compliance assurance.

- We employ a unified governance framework for all cybersecurity initiatives.
- Align cybersecurity programs with enterprise priorities, regulatory mandates, and risk strategies.
- Enable executive oversight through steering committees, OKRs (Objectives and Key Results), KPIs (Key Performance Indicators), and decision forums.

Benefits

This service is particularly beneficial for organisations wanting:

- Strategic Alignment: Ensuring every cybersecurity initiative supports enterprise objectives and risk priorities.
- Increased Accountability: Clear governance and reporting, providing transparency for executives and regulators.
- Operational Efficiency: Streamlined coordination, reducing duplication and accelerated delivery.
- Enhanced ROI: Focused investment management to minimize risk and business impact.
- Predictable Outcomes: Consistent methodologies delivering programs on time, with predictable outcomes and measurable results.

What's included in the Dev/Null service?

Objectives Defined:

An in-depth assessment of the programmes / project's goals and how it aligns with business strategy whilst supporting enterprise objectives and risk priorities This phase gathers all relevant information to form a complete picture of your project requirements.

Scope Creation:

A detailed document detailing the full scope and list of deliverables within the cybersecurity initiative.

Facilitate Collaboration and Communication:

Ensures stakeholders are aligned.
Facilitate data-driven decision-making and early issue escalation.
Provides a framework for regular progress updates and reporting from business case to benefits realisation.

Programme / Project Plan:

A structured roadmap for planning, executing, and managing a cybersecurity initiative, outlining the timeline, milestones and deliverables, and resources are properly allocated.

Identify and Manage Risks:

Embed risk management practices within project governance and delivery processes.
Anticipate potential cybersecurity threats or project risks (e.g., delays, resource shortages, vulnerabilities).
Includes strategies for risk mitigation and incident response during implementation.

Measure Success:

Defined OKRs, KPIs and metrics to facilitate cybersecurity objectives being met.
Alignment with cybersecurity standards, legal obligations, and organizational policies.
Conduct a benefits realisation review.

Adoption:

Drive cultural adoption of cybersecurity initiatives across your business.
Manage communications, training, and stakeholder alignment to ensure sustainable change.
Enable transparency and accountability through clear roles, responsibilities, and communication plans.

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.

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.

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.

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.

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.

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

Choosing the right partner for your Cyber PMO Service is crucial. At Dev/Null, we combine decades of collective Cyber PMO and cybersecurity experience to deliver programs and projects tailored to your organization's needs. Our team brings expertise from diverse industries and across all aspects of cybersecurity - from design and build to operate and evolve. We leverage our deep understanding of industry best practices, combined with hands-on operational experience, to drive real improvement in your security posture.

Book a conversation with one of our consultants to explore how our Cyber PMO service can help you deliver.

info@devnullsecurity.co.uk