

# Chief Information Security Officer-as-a-Service



## Cost-effective cyber & information security management

PGI's Chief Information Security Officer-as-a-Service (CISOaaS) offering provides organisations with cyber and information security leadership, and the knowledge and expertise of a CISO without the high-cost investment of a full-time resource.

By choosing to implement a CISOaaS approach, you'll be taking advantage of the expertise and specialist skillsets of PGI's team of information and cyber security experts to manage risk and improve your organisational security posture. This ensures that cyber-related risks are identified, understood and mitigated to an appropriate level based upon the organisational appetite for risk.



### A fully tailored approach

PGI's CISOaaS is a tailored three-stage approach to ensure your organisation's strategy is implemented effectively. This process provides the necessary management information to assess, understand, implement and ultimately maintain a mature security posture appropriate to your organisation's threat profile and risk appetite.



#### PHASE 1: ONBOARDING

In the onboarding phase, our experts will undertake a maturity model to gain an in-depth understanding of your cyber security posture—a comprehensive view of policies, processes, procedures, cultural security awareness and technical controls.

Because this phase provides insights into your organisation's security strengths and weakness and therefore a view of your risk profile, it will help dictate what the next two phases look like and where investment should be focused. We'll provide an initial risk register (or update existing documentation) and plan for the work required to reduce the gaps identified in current security measures.

Importantly, you will be provided with an in-depth report that can be used to communicate your organisation's requirements to Executive and Board level management in a clear and concise format. This report will enable buy-in by providing leadership with a non-technical appraisal of the risks and mitigation strategies.



## PHASE 2: IMPLEMENTATION

The findings from phase one will inform the cyber security management strategy best suited to your organisation's needs. Based on this, PGI will provide the appropriate expertise for the areas in which investment should be focused, such as risk management, audit, documentation and incident management.

PGI subject matter experts will support—or in many cases create and deliver—the required policy sets, procedures, corporate awareness materials, and act in a technical advisory capacity.

By the end of the implementation phase, you will have in place a comprehensive cyber security strategy; PGI will have advised and supported delivery throughout, culminating in a successful implementation.



## PHASE 3: MAINTENANCE

In the final phase of the process, our experts will maintain the improved security position through annual audits and testing, as well as remaining up-to-date with the relevant regulation requirements. Importantly, because of the policies, procedures and governance developed during the first two phases, ongoing compliance—to regulatory, internal or customer demands—is far less resource-intensive.

### Is CISOaaS right for your organisation?

In the UK alone, there is a huge shortage of information security professionals. Globally, the estimated shortfall of security personnel is an estimated 3.5 million. This drives up the salary levels of cyber and information security experts, which is why many organisations are looking to the support of a partner in the delivery of security management and CISO capability.

If you know you need to make improvements to—or put in place—cyber security measures, but don't have the resource or expertise, a good starting point is the adoption of CISOaaS. You'll have access to a pool of experts for the price of less than one.

### Why choose PGI's CISOaaS offering?



**Significant cost savings** - Because our CISOaaS offering is tailored, your organisation only needs to invest in what is needed.



**Vendor-neutral advice** - PGI are vendor-neutral, so we will always act in your best interests when assessing your risks and offering a solution.



**Flexibility** - We know the cyber threat is constantly evolving so we work to your needs and business requirements.



**Increased management engagement** - Our team have long experience in concisely communicating security matters to all levels of executives, board members and non-technical senior staff.



**Subject matter expertise** - Undiluted focus on building cyber security capacity and capability, and access to a diverse array of technical and non-technical cyber security skills.



Are you ready to take control of your cyber security?

Contact us to discuss your requirements and how we can help you protect your people and assets

@ clientservices@pgitl.com 0845 600 4403 pgitl.com