CYBER ASSURANCE AS A SERVICE

Outsourced cyber security management

Effective cyber assurance is a combination of human and technical measures that grow with your organisation. But finding the right internal team to direct and implement any of these measures can be a tough, time-intensive and expensive task.

That's why there are many benefits to outsourcing cyber security management, including:

- Access to a full team of information and cyber security experience, without the headcount or recruitment costs.
- No lengthy recruitment and onboarding process, which means immediate action.
- Unbiased and vendor independent views of security controls.

In addition, PGI's Cyber Assurance as a Service provides you with what your organisation needs, not a one-size-fits all solution. Depending upon your cyber maturity, we can offer specific streams of activity that focus on security stakeholder management, foundational security governance, improving an existing framework, or keeping it all compliant. Or, we can do it all!

HOW PGI CAN HELP YOU MANAGE YOUR CYBER SECURITY

No organisation is exactly the same, which means a blanket information and cyber security approach is not suitable. Our Cyber Assurance as a Service is a holistic approach that ensures each of our clients is getting the right level and type of support.

Virtual CISO - The CISO function provides strategic direction and an open communication channel to stakeholders, to ensure that cyber security has representation at executive level. Finding the person with the right experience can be time-consuming and expensive. With PGI's Virtual CISO service option, your organisation benefits from a team's worth of expertise immediately, not just one expensive individual, to provide security leadership and strategic advice.

Gap Assessments - Understanding the current status of your cyber security is the first key step that a CISO will look to establish, in order to develop a route map for your subsequent actions. Our consultants review your organisation's current security measures and—taking into account any specific aims or regulatory requirements—provide practical and necessary assistance on where improvement efforts will be needed. Depending upon the size of your company, and its certification ambitions, this can be an assessment against a range of different security baselines (see on the next page for examples).

Governance Focus - A strong cyber security strategy has a strong foundation. PGI's consultants can help your organisation develop foundational security governance measures that will form the basis of your information security framework. Typical deliverables to establish your information security framework (ISMS), may include, establishing roles and responsibilities, setting up governance forums, undertaking security risk assessments, and developing initial policies.

Tune-Up Focus - Failure to properly embed controls into business processes can result in non-compliance, leading to data breaches and enormous reputational damage. This stream builds upon and improves your ISMS. PGI's consultants can develop an extended range of policies; progress key processes such as supplier assurance, business continuity, and vulnerability management; provide direction and assistance for addressing specific information assurance concerns, such as data loss prevention, or achieving ISO 27001.

Review Focus - Information and cyber security controls are not 'set and forget' and should always be subject to review and continuous improvement. PGI's experts will help you establish strong compliance processes which includes developing effective metrics reporting, performing internal audits and controls testing to ensure measures continue to be effective and compliant.

WHY OUTSOURCE YOUR CYBER SECURITY TO PGI

Engaging PGI to manage your cyber security means your organisation has access to the experience of a full team of information security experts, along with the skills of our wider technical team if required.

Without the lengthy recruitment process and head count increase, our team can make an immediate difference to your organisation's cyber security.

Our Cyber Assurance as a Service is a structured, holistic approach that focuses on getting cyber security controls right, specifically for your organisation and then ensuring continued improvement.

OTHER PGI SERVICES

Since 2013, PGI has been helping organisations of all sizes achieve compliance with a range of frameworks, including GDPR/The Data Protection Act, ISO 27001 and PCI DSS.

We also offer a wide range of cyber security services, including vulnerability assessments and penetration testing to further support effective data protection.

Understanding the threats that your organisation and industry are up against will help you defend your data, infrastructure and reputation. Talk to our team to discuss your cyber and information security needs and how we can help.

CYBER ASSURANCE AS A SERVICE

PGI can provide all aspects of this service as a virtual / remote solution using our available collaboration platforms and tools; and using our flexible and experienced consultants.

CISO FOCUS	GAP ASSESSMENT	GOVERNANCE FOCUS	TUNE-UP FOCUS	REVIEW FOCUS
What is this service?				
This stream focuses on filling the increasingly needed role of a Chief Information Security Officer (CISO). The CISO role has a wide range of priorities, including stakeholder management, communication and advice across the business, and managing resources to ensure delivery. In addition, the CISO provides security oversight, understands and designs security architecture best practices, and develops an integration of security with business aims and risk appetites. It coordinates, drives change, and control deployment, potentially making use of the 3 other focuses (Governance, Tune-up, and Review).	Gap assessment reviews the current status of cyber security in your organisation. Depending upon your considered objectives and the size / complexity of your company, this can be completed against a number of different methods: • ISO 27001 / ISO 27002 standards • Cyber Maturity Model • 10 Steps to Cyber Security (NCSC)	This stream focuses on setting up a foundational baseline of security governance measures to establish your information security framework. It concentrates on developing a range of typical governance-related priorities and deliverables. For example: • Establishing roles and responsibilities • Basic staff awareness and training • Core security policies • Security risk assessment process	This stream focuses on building up and improving existing information security controls, particularly around fine-tuning and documenting processes that are critical for good security practice. For example: • Change management • Incident response • Access control • Supplier assurance PGI's team can develop an extended range of policies and provide direction and assistance for establishing specific goals, such as data loss prevention.	This stream focuses on ensuring continuous improvement is made towards an established and maturing security framework. It concentrates on carrying out compliance review processes; as well as establishing the capability for monitoring and measuring the effectiveness of security control implementation. For example, performing regular internal audits, producing KPI dashboards, testing incident response plans and performing annual policy reviews.
Why do you need this service?				
The CISO function that will identify risk issues with a focus on protecting information assets, and the business value chain. The CISO should direct the all-important cyber and information security strategy and be a trusted advisor with open communication channels with leadership. Key deliverables include the development of a Security Strategy with an accompanying Roadmap. The function is also important for the process of communicating cyber risk to organisation management in order to elicit buy-in and support.	It helps you to define your security requirements and what subject areas and aspects of cyber security should be concentrated upon. Depending on the outcome of the assessment (embryonic, developing, or ongoing and mature) this will illustrate which of the focus streams should be engaged.	In order to construct a robust and sustainable security framework, strong foundations are required, including establishing top management/ leadership support and commitment, ensuring that there are appropriate resources (budget and people), and putting in place the initial building blocks.	Failure to embed ongoing measures after initial establishment of governance means that your security framework could potentially stutter and stall. This could result in data breaches and subsequent fines or penalties, as well as enormous reputational damage. This stream has a strong focus on developing 'business as usual' security processes that can be consistently implemented.	To effectively manage a security control, you must be able to measure its effectiveness. This stream will ensure that your all-important audit and review processes and testing and monitoring capabilities are established, optimised, and management has visibility of their results.
What are the benefits of this service?				
PGI can provide this cyber security leadership and trusted advisor role from a pool of experienced consultants and practitioners. We will build and supply a service that will be tailored to fit your business needs, while you gain access to the full spectrum of PGI's skills and knowledge.	The gap assessment provides a view of where effort needs to be concentrated to ensure progress, and which actions should be performed first. This can help with project planning, resource forecasting and budgeting. You will be provided with a detailed Gap Assessment report, describing the findings and prioritised recommendations.	Often, not knowing where to start can hinder the embedding of information governance, but PGI's team of experts can help you establish strong security governance controls. If your organisation is aiming for ISO 27001 certification this will launch your implementation by focusing on the first four sections of the standard (Context / scope, Leadership, Planning, and Support). If you are aiming to improve your cyber maturity in general, then this stream will assist greatly with moving from initial Levels (0-1) and progressing to maturity Level 2+.	With PGI's support, your organisation can be assured that implemented control measures are pragmatic and provide the appropriate levels of assurance. PGI consultants can apply their expertise to develop policies and procedures tailored to your business, allowing your workforce to focus efforts on other implementation activities. For ISO 27001 ambitions, this stream focuses on building your documented information and improve security operations. Cyber maturity will be lifted to Level 3. PGI can also perform penetration tests, vulnerability assessments, or fulfil targeted security training as required.	PGI's experts can help you establish strong security review and monitoring controls. For an ISO 27001 concentration this will include an emphasis on Information Security Management System (ISMS) performance evaluation, corrective action tracking, and continual improvement. For cyber maturity improvement, this stream will assist with moving beyond a maturity Level of 3.
How long will it take?				
PGI can provide you with a CISO service that will show immediate benefits, because you won't need to consider a lengthy recruitment and onboarding process. Dependent on how many days per month are established as a requirement (from 2 days up to 30 days), the CISO service could be looked upon as an ongoing investment that will continue to demonstrate great ROI over the full calendar year.	This depends on the size of the organisation, the complexity of its IT and Network infrastructure and business processes, and the company's objectives. 10 Steps review: Approx. 5 – 7 days ISO 27001 / ISO 27002: Approx. 6 – 10 days Cyber Maturity review: Approx. 8 – 15 days	There are several factors that can influence the timescales required to establish good security governance practices in an organisation. These can include the company culture, management support and availability of resources. Typically, you should expect a successful implementation to take between 6-8 months.	Factors that can influence timelines for the successful implementation of this stream are similar to those in the 'Governance Focus'. Other key factors are your organisation's appetite for change and ability to move at a pace which does not disrupt and impact the business. Approx. 6-8 months.	It is important to establish review processes that—whilst carried out regularly—do not significantly impact on business resources or systems. Implementing successful processes in this stream, should be scheduled across the year and, on average, should take 6-8 months to initially establish.
Why do I need PGI's help?				
Effective individual CISOs can be hard to find and very expensive. Rather than delay establishing or upgrading your cyber security strategy, your organisation can make use of PGI's pool of resources to start laying the foundations for a permanent in-house function or, as an alternative, a cost-effective ongoing managed solution without needing to open up new internal positions.	Expertise in cyber security allows PGI's consultants to accurately assess your organisation's current levels of maturity and provide pragmatic recommendations. With the help of PGI's trained assessors, a gap analysis can be performed more efficiently and effectively than by internal staff, who are likely to hold other responsibilities, and may not be as familiar with the intricacies of cyber security best practices.	Engaging PGI means you can take advantage of a team of practised consultants means who, between them, have decades of security knowledge, qualifications and skills honed in frontline security positions across a range of diverse industries and sectors. From day one, your organisation can tap into and benefit from this expertise rather than potentially delaying your requirements via the costly development of in-house staff or running an exhausting recruitment campaign.	It may be the case that your organisation is best placed to perform much of the implementation. However, PGI are well-placed to provide bespoke support and advise where specialist expertise is very often necessary, and where your organisation lacks the appropriate resource. Engaging with PGI enables an independent and unbiased view of the suitability of security-related controls and processes that need to be implemented.	PGI can provide skilled and knowledgeable audit practitioners. Our security consultants also have deep experience of implementing controls that ensure continuous improvement of an ISMS. As for the other streams, you will be immediately procuring ready-made security skills and knowledge versus potential delays and frustrations encountered by developing the required in-house skills or external recruitment.

WHY OTHER ORGANISATIONS CHOOSE PGI

PGI is a UK-based risk mitigation consultancy with key services across risk analysis, cyber security, intelligence and training. We believe that cyber and information security don't need to be overly complicated, incomprehensible or vastly expensive.

A tailored approach
Not every business is the same, so we don't attempt to approach every project in the same way. We get to know your organisation, so we can provide appropriate advice.

Practical and affordable
Solutions are affordable because they are proportionate only to a client's needs, not a blanket approach.

Cross-sector experience
PGI are made up of personnel with backgrounds in cyber and information security, law enforcement, intelligence, the military and academia and have implemented information security measures across a wide range of industries.

Global experience
PGI have worked with companies in more than 50 countries.

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

+44 (0) 845 600 4403
sales@pgitl.com
www.pgitl.com