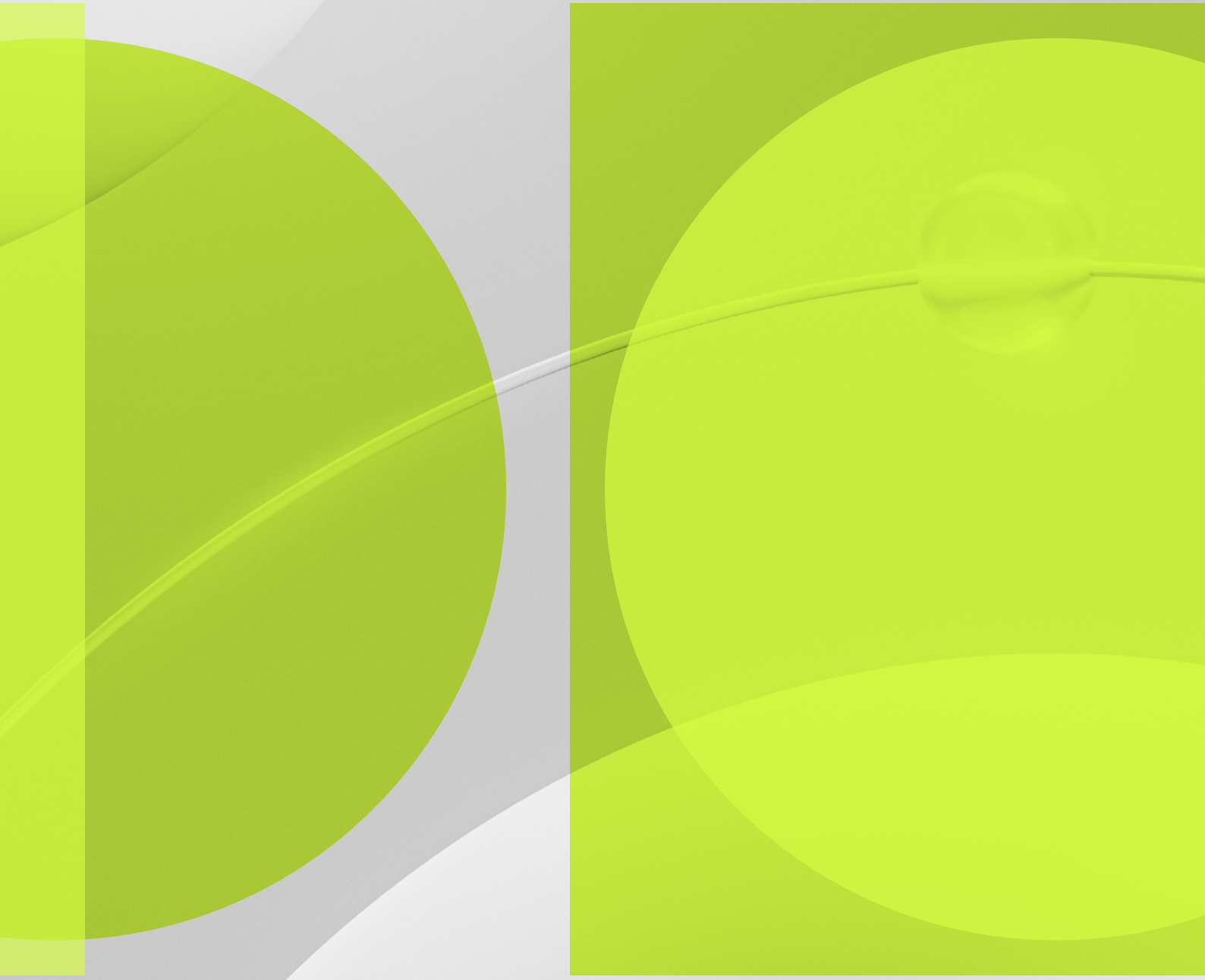
Cyber Assurance as a Service

Introduction 2

How we can help 3

Why outsource? 4

Services menu 5



Visit: www.pgitl.com
Email: sales@pgitl.com

Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V

Protection Group International Ltd
Registered in England & Wales, 07967865

Cyber assurance is about being confident that your security controls will meet risk thresholds. Recruiting an internal team to implement specialised cyber security measures can be time-consuming, difficult and expensive. Fortunately, outsourcing your cyber security to PGI brings a range of compelling advantages...

When you outsource your organisation's cyber security to PGI, you'll benefit from having access to a complete team of information and cyber security experts, all without the need for additional headcount or incurring recruitment costs. Our services ensure immediate action to secure your systems and processes effectively. Moreover, you'll receive unbiased, fully independent advice on security controls, leading to the implementation of optimal solutions tailored to your specific needs.

At PGI, our Cyber Assurance as a Service assesses what your organisation needs and tailors a bespoke solution. Depending on a client's cyber maturity, we offer four streams of activity:

1 SECURITY STAKEHOLDER MANAGEMENT

2 FOUNDATIONAL SECURITY GOVERNANCE

3 IMPROVING AN EXISTING FRAMEWORK

4 KEEPING A FRAMEWORK COMPLIANT

Helping you manage every element of your cyber security

Each organisation is different, so a one-size-fits all approach to information security tends to lack precision and effectiveness. At PGI our fully customisable Cyber Assurance as a Service establishes your organisation's needs and provides an ideal level of support. Matching your needs at every stage, we offer the following services:

1

SECURITY STAKEHOLDER MANAGEMENT

VIRTUAL CISO: Our Chief Information Security Officer (CISO) will provide your organisation with strategic direction, and ensure that cyber security is represented at executive level. Choosing a Virtual CISO will bring you instant, outstanding security leadership and an entire team's worth of expertise.

GAP ASSESSMENTS: We will establish the status of your cyber security and develop a roadmap for subsequent actions. This roadmap will fulfil your organisation's specific aims, and comply with regulatory requirements. Depending on the size of your company and its certification ambitions, we assess against a range of security baselines.

2

FOUNDATIONAL SECURITY GOVERNANCE

GOVERNANCE: All successful cyber security strategies rely on good governance. Our consultants will help you develop and embed strong governance measures that will form the foundation of your Information Security Management System (ISMS).

3

IMPROVING AN EXISTING FRAMEWORK

TUNE-UP: This service builds on and improves your existing Information Security Management System. This helps guarantee compliance, avoid data breaches and reputational damage. We can assist in developing an extended range of policies, progressing key processes, and achieving ISO 27001.

4

KEEPING A FRAMEWORK COMPLIANT

REVIEW: In the fast-moving digital realm, information and cyber security controls are not 'set and forget'; they should always be subject to review and continuous improvement. Our experts will help you establish strong compliance processes, including metrics reporting, internal audits and controls testing to ensure measures continue to be effective and compliant.

Why outsource your cyber security to PGI?

We believe that exceptional cyber and information security doesn't need to be overly complicated, or vastly expensive. Our dedicated personnel are globally respected cyber-security experts and thought-leaders, with backgrounds in security, law enforcement, the military and academia.

We have worked with organisations and institutions in more than 50 countries worldwide and implemented security measures across a wide range of sectors and industries.

When you work with PGI, you gain access to the experience of our information security specialists, along with the skills of our wider team. We will make an immediate difference to your organisation's cyber security – while you avoid a lengthy recruitment process and head count increase.

PGI's Cyber Assurance as a Service offers a flexible approach that focuses on getting cyber security controls right, and ensuring continued improvement. Solutions are affordable because they are proportionate to your needs.

We're vendor-neutral, always acting in organisations' best interests when assessing risks and offering solutions.

Visit: www.pgitl.com
Email: sales@pgitl.com

Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V

Protection Group International Ltd
Registered in England & Wales, 07967865

Flexible expertise, at your service

Our experienced consultants can provide all aspects of the Cyber Assurance Service as a virtual/remote solution, using our collaboration platforms and tools. Browse the table below to see the full menu of services and their benefits.

ACTIVITY STREAM	SECURITY STAKEHOLDER MANAGEMENT 1		FOUNDATIONAL SECURITY GOVERNANCE 2	IMPROVING AN EXISTING FRAMEWORK 3	KEEPING A FRAMEWORK COMPLIANT 4
Service title	Virtual CISO	Gap assessment	Governance	Tune-up	Review
What is this service?	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 other PGI services (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 + 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 a range of policies and provide direction 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. This includesthe establishment of 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. For ISO 27001 certification, we focus on the first four standard sections: 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 organization can implement pragmatic control measures with confidence. Our consultants develop tailored policies and procedures, freeing your workforce for other activities. For ISO 27001, we focus on building your documented information and enhancing security operations, lifting cyber maturity to Level 3. PGI also offers penetration tests, vulnerability assessments, and targeted security training as needed.	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 inhouse 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 wellplaced 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 securityrelated 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.