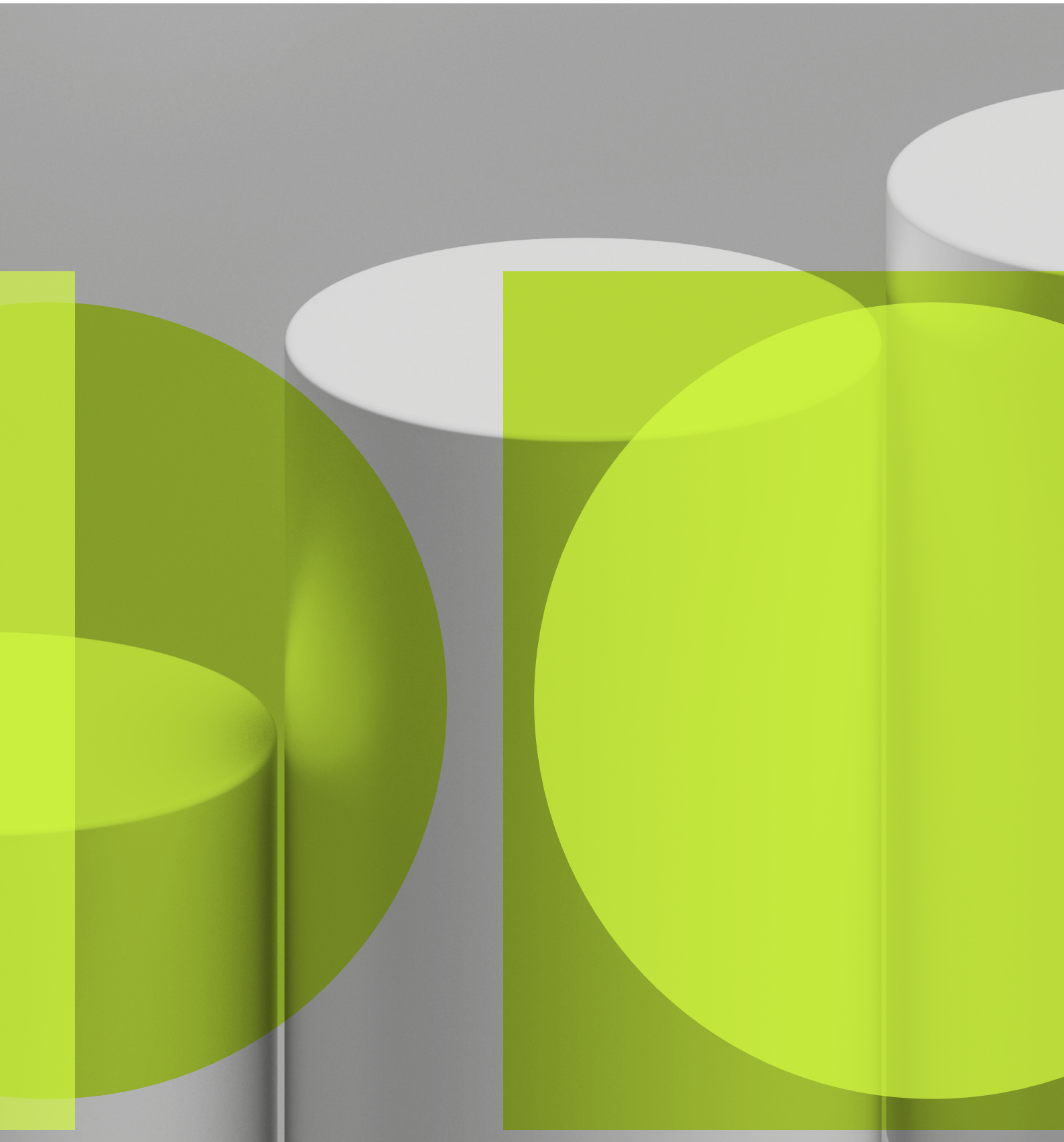
When your organisation needs to be PCI DSS compliant



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

Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT

Protection Group International Ltd
Registered in England & Wales, 07967865

Payment card security is one of the most important security concerns for consumers and businesses.

PCI DSS compliance demonstrates that your business uses the confidential payment data of your customers in a safe and secure way, minimising risks associated with payment card fraud.

According to the Department for Digital, Culture, Media and Sport, just 37% of businesses have policies in place to control important security requirements, such as data encryption. With the rise of the digital economy and online businesses, it's crucial to have the right security controls in place to ensure customer payment information is secure.

What is PCI DSS?

Payment Card Industry Data Security Standard (PCI DSS) is a set of mandatory security requirements that must be adhered to by any business (merchant or service provider) which stores, processes or transmits payment card data. The business must attest their compliance with the standard on an annual basis.

How we can help

Outsourcing your PCI DSS compliance requirements provides peace of mind and ensures internal staff can concentrate on your core operations. We can scope your requirements, identify areas that require improvement, implement security measures, undertake auditing and reporting functions, and help you remain compliant.

Regardless of its current position on the PCI DSS journey, we will support your organisation to meet compliance needs:

SCOPE VALIDATION

A scope validation ensures your organisation has correctly evaluated in-scope systems, people and processes. Conversely it can also confirm that you are not over-reporting, which saves time and reduces costs. Our team can provide expert validation of compliance scope, assessment for scope reduction, Self-Assessment Questionnaire (SAQ) determination, and employee awareness and training sessions.

GAP ANALYSIS

Understanding where your organisation currently sits with respect to PCI DSS requirements can be used to facilitate effective project planning, resource forecasting and budgeting. We can undertake a gap analysis to gain an in-depth understanding of where efforts should be focused, by reviewing existing policies, processes, and controls relevant to the cardholder data environment.

IMPLEMENTATION

Assistance from an external Qualified Security Assessor (QSA) to implement PCI control measures ensures that the measures are pragmatic and appropriate. Our team can put in place—or help your team put in place—the control measures that ensure compliance with PCI DSS.

AUDIT AND COMPLIANCE REPORTING

We can support your organisation with the completion of the required reports—either SAQs or a full QSA-led Report on Compliance (ROC). This ensures peace of mind, particularly around the credibility of the content.

STAYING COMPLIANT

To reduce the likelihood of 'next year non-compliance' syndrome our PCI DSS experts can assist you with maintaining and continuously improving security. To remain PCI DSS compliant, companies must complete mandatory testing, which we can provide. This includes internal vulnerability assessments as well as internal and external penetration testing and segmentation testing. We can also review business or system changes and the impact these have on your PCI scope and reporting requirements.

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

Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT

Protection Group International Ltd
Registered in England & Wales, 07967865

Why choose PGI

We are a UK-based risk mitigation consultancy empowering organisations to counter digital threats. Our experts help organisations build digital resilience and 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

Our solutions are affordable because they are proportionate to your needs, not a blanket approach.

CROSS-SECTOR EXPERIENCE

Our team are made up of personnel with backgrounds in security, law enforcement, intelligence, the military and academia and have implemented information security measures across a wide range of industries.

VENDOR-NEUTRAL ADVICE

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

Your map to PCI DSS Compliance

SCOPE VALIDATION	GAP ANALYSIS	IMPLEMENTATION	AUDIT & COMPLIANCE REPORTING	CONTINUOUS IMPROVEMENT

What is this service?

Many organisations begin with a gap analysis or implementation, but we believe that a scope validation is the best starting point; it determines which systems, personnel, locations, and processes form the Cardholder Data Environment (CDE) and what must be compliant with PCI DSS.

Gap analysis involves comparing what you are currently doing against what you must do to meet PCI DSS compliance requirements.

Implementation focuses on putting in place control measures to ensure PCI DSS compliance.

Our team will provide expertise in the appropriate implementation of controls.

Audit and Compliance Reporting involves reviewing the implemented controls and reporting your compliance with PCI through the appropriate mechanisms.

Continuous improvement is all about maintaining your compliance with PCI DSS, especially in light of changes to the CDE.

Why is it important?

It helps you to define your CDE and to establish your PCI DSS reporting requirements (e.g. which Self-Assessment Questionnaire (SAQ) to complete). The standard states that this should be done on an annual basis.

It informs where there are shortfalls in compliance and where efforts must be concentrated to meet the requirements of the standard.

Failure to implement the necessary controls means the organisation is not compliant. This could result in data breaches and subsequent fines or penalties, as well as significant reputational damage.

In the event of a breach, organisations that do not comply with the relevant regulations are likely to be fined at a higher rate.

Organisations must report their PCI DSS compliance status. The amount of card transactions processed each year will dictate how your organisation must report its compliance. This will be either:

- Report on Compliance (ROC) + Attestation of Compliance (AOC)
  OR
- Self-Assessment Questionnaire (SAQ) + Attestation of Compliance (AOC)

It reduces the likelihood of 'next year non-compliance' syndrome.

Organisations must maintain their compliance with PCI DSS and report their compliance status annually. This may include performing regular vulnerability assessments and penetration tests and implementing an ongoing security awareness programme.

Any changes to the CDE must be considered and appropriately reported. For example, introducing a new payment channel may affect which SAQ(s) must be completed.

SCOPE VALIDATION	GAP ANALYSIS	IMPLEMENTATION	AUDIT & COMPLIANCE REPORTING	CONTINUOUS IMPROVEMENT

What does your organisation get from this service?

Factors including the number of transactions and how the organisation processes card payments will impact your reporting requirements. Scope validation ensures that you are not over-reporting, saving time and reducing costs.

We will provide a comprehensive report detailing the CDE and your reporting requirements (e.g. which SAQ to complete).

The gap analysis provides a view of where effort needs to be concentrated to ensure compliance, and which actions should be prioritised. This can facilitate effective project planning, resource forecasting and budgeting.

You will be provided with a detailed PCI Gap Analysis Report, detailing the findings and prioritised recommendations. We will also document the evidence reviewed helping to streamline compliance reporting at a later stage.

With our support, you can be assured that control measures implemented are pragmatic and provide the appropriate levels of assurance.

As an example, our consultants can apply their expertise to develop PCI compliant policies and procedures, allowing your workforce to focus efforts on other implementation activities.

Our wider team can also perform penetration tests and vulnerability assessments as required by PCI DSS.

PGI is approved as a PCI Qualified Security Assessor (QSA) company and can be engaged to audit your controls and help complete ROCs, SAQs and AOCs.

A ROC and its associated AOC must be completed by a PCI QSA.

A SAQ and its associated AOC does not need to be completed by a QSA, but using a QSA can provide greater credibility.

We provide ongoing PCI compliance support, including expertise on how to improve security controls, as well as reviewing any business changes and their impact on your PCI compliance and reporting obligations. We can also provide:

- Regular security audits (quarterly targeted control reviews are recommended)
- Regular newsletters informing on changes and trends
- Penetration Testing
- Vulnerability Assessment
- Security awareness and education

How long will it take?

This depends on the size of the organisation and the complexity of its payment processing methods.

Approx. 1 – 2 days

This depends on the size of the organisation and its reporting requirements e.g., against which SAQs or a Report on Compliance (ROC), that the gap analysis is to be performed.

Approx. 8 – 10 days

This is heavily dependent on your organisation's current levels of compliance. Establishing a timescale can be very difficult, which is why PGI recommends performing a Gap Analysis. The findings of the Gap Analysis can be used in project planning and resource forecasting.

Approx. 3 – 10 months

This is directly impacted by the PCI reporting requirements of your organisation. For example, completion of a ROC or SAQ D, will take longer than an SAQ A-EP.

Approx. 2 - 3 days

For all ongoing support, we will provide clear timescales, considering the size of the organisation and complexity of its CDE.

Why do I need PGI's help?

We provide reassurance that your organisation is meeting its PCI reporting obligations.

Our consultants can also advise on operational changes and scope reduction where applicable. This may significantly reduce your PCI reporting requirements.
Typically scope validation is carried out by a Qualified Security Assessor (QSA).

Our consultants' expertise in PCI DSS mean they will accurately assess your organisation's current levels of compliance and provide pragmatic recommendations.

Our consultants can perform a gap analysis 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 the standard.

It may be the case that your organisation is best placed to perform much of the implementation. However, where necessary, we can provide support and advise where specialist expertise is necessary, or where your organisation lacks the appropriate resource.

Engaging us allows an independent and unbiased view of the suitability of the controls being implemented.

If you are not fully confident in completing an SAQ, or if you come up against time and resource constraints, we can help. Engaging with one of our QSAs will ensure that your SAQ is completed efficiently and with the appropriate level of detail.

If a ROC is required, then a QSA must be employed to audit your controls and complete the necessary reporting.

Our expertise and experience can help you devise an effective continuous improvement programme that is appropriate for your organisation. PGI consultants provide you with specialist knowledge and resource capacity, enabling your workforce to concentrate on core operations.

Our QSAs have an extensive understanding of PCI DSS and can ensure any business changes are completed in a compliant manner.

Visit: www.pgitl.com
Email: sales@pgitl.com
Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT
Protection Group International Ltd
Registered in England & Wales, 07967865