How well is your organisation set up to manage cyber risk?

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

Our cyber security maturity assessment will help you understand and improve your organisation's security position.

Cyber threats vary between different companies and different sectors, so 'a one size fits all' approach to cyber and information security doesn't work, and can be very costly. Understanding your position will highlight areas for improvement and priority of the investment required to keep your data and reputation safe.

Our Cyber Security Maturity Assessment analyses current security measures to establish effectiveness. They are evaluated against organisational maturity targets, based on risk appetite, stakeholder expectations, and regulatory/legal requirements. This enables us to provide a tailored service which suits your specific needs.

We believe that there's no point allocating excessive budget to something if it's not required.

What is a Cyber Security Maturity Assessment?

The maturity assessment involves comparing your organisation's current security measures against the criteria of our Cyber Security Maturity Model, which is based on a wide range of security industry standards and best practices, such as:

- ISO 27001
- PCI DSS
- NISD
- GDPR
- CIS

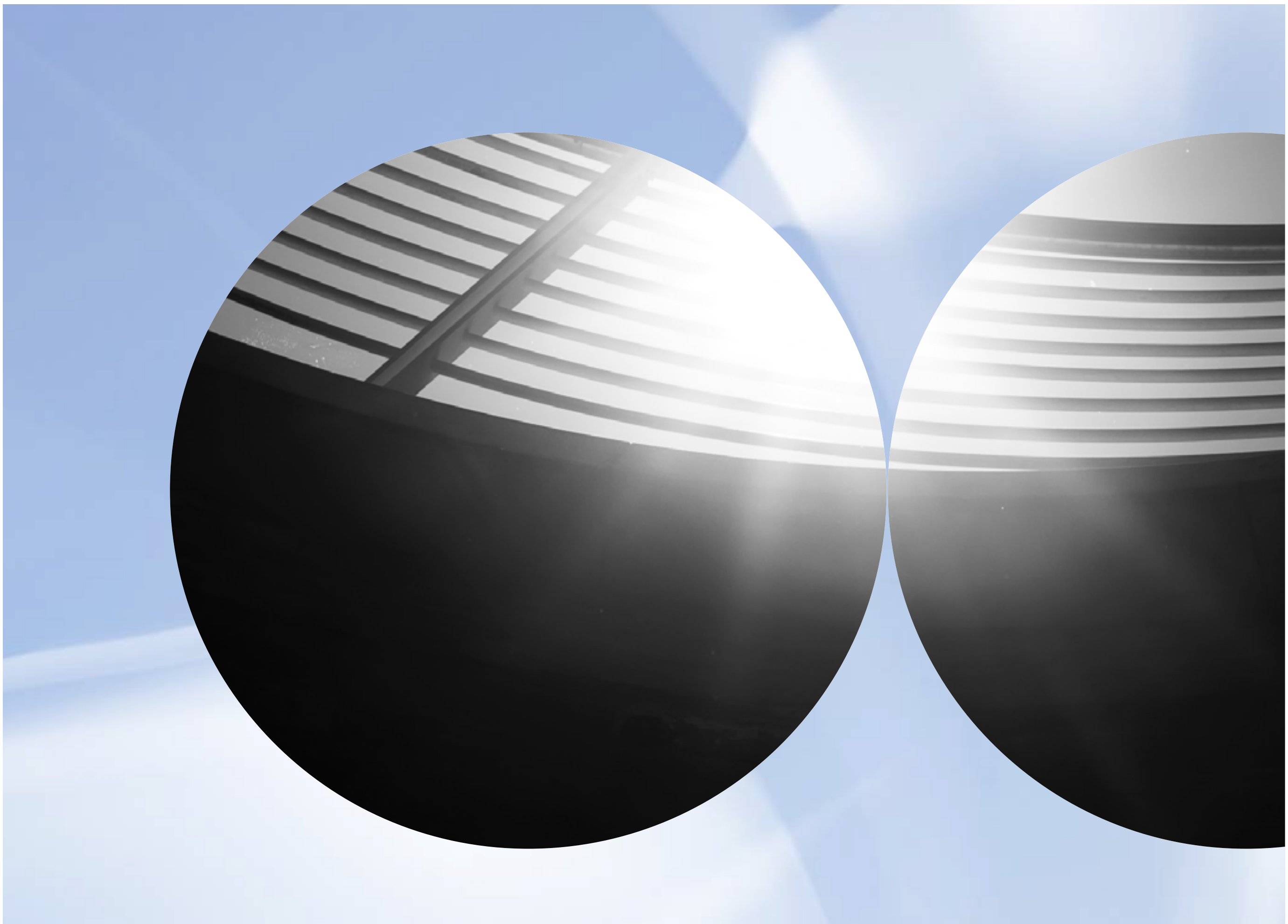
Out consultants will evaluate 139 data points (processes, policies, and controls) within 15 key business areas which have a bearing on your company security posture, covering technology, people, processes, and physical security. They score these using a 6-point scale that ranges from 0 (non-existent) to 5 (optimised).

From this, the maturity of your organisation's security posture and the status of each core individual subject area can be analysed and areas for improvement identified.

You can choose to perform a full cyber security maturity assessment (approximately 3-20 days) or a partial assessment, selecting the most pertinent areas (e.g., Network Security and Business Continuity).

If your organisation does not have any specific regulations to comply with, the maturity assessment will provide a strong all-round view of security best practice.

With this model, we can provide you with a clear way to see where your organisation needs to mature and to decide what maturity level is acceptable. It also provides a clear way to monitor and demonstrate progress if the CMM is repeated (e.g., annually), through use of an informative and consistent maturity scale across different areas of information security.



The benefits of assessing your cyber security maturity

The assessment provides an in-depth and balanced view of your organisation's preparedness against cyber threats and your ability to protect your information assets.

Understand the gaps in your processes

Our assessment identifies where security measures are less mature than industry accepted good practice and where efforts must be concentrated to improve your organisation's posture. You should consider undertaking a cyber security maturity assessment if you want to:

- Create a stronger security culture
- Ensure that your organisation is prepared to face the evolving security threat landscape
- Understand what actions must be undertaken to improve your security

Our consultants are external to your organisation, so you can be assured of an independent and unbiased view of current maturity levels and recommended actions.

Prioritise investment in security measures

Your report will detail the findings, evaluated maturity levels and recommendations. These findings will shape how effort is concentrated to improve maturity levels and which actions should be prioritised. This can facilitate effective project planning, resource forecasting and budgeting, and will provide you with a cyber strategy planning tool to ensure that your team target the right amount of maturity for areas that can create improvement and protect valuable assets.

Facilitate communicating cyber security and information security to management

It is becoming increasingly common that executives must reassure and actively provide evidence of appropriate information management safeguards to customers and stakeholders. We provide your key decision makers with an independent, non-technical explanation of the current cyber maturity levels and recommended actions, in-line with your organisation's risk appetite and desired maturity.

This business-focused approach ensures all important messages can be readily understood across the organisation. On request, our experienced consultants or CEO can provide a briefing (maximum two hours) to your Senior Leadership Team, where we will summarise the findings of the assessment and discuss our recommended actions. This briefing provides your Senior Leadership Team with a clear understanding of your organisation's cyber security maturity and where improvements must be made.

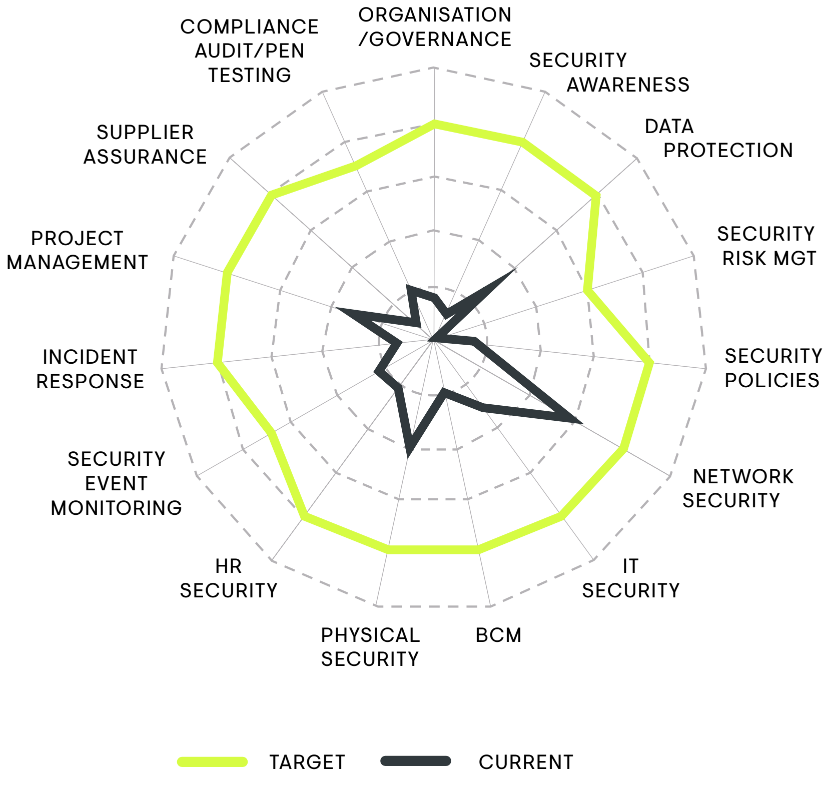
Facilitate continuous improvement

Continuous improvement is an important aspect of remaining compliant with a number of regulations; this is why many organisations find benefit in repeating these assessments at regular intervals (e.g., annually). This provides a consistent metric for key stakeholders to measure and demonstrate continuing improvement and increasing maturity levels.

Why work with PGI to understand your cyber security maturity?

Our Cyber Security Maturity Model has been designed to cover the many cyber security and compliance requirements of your business. The expertise of our consultants in cyber security, information security frameworks, and maturity assessments means they can accurately and independently assess your organisation's current cyber maturity levels and provide pragmatic recommendations.

Current Status - Sorted by Subject Area vs. Target



Cyber Security Maturity Model Areas of Review

ORGANISATION/GOVERNANCE

Includes:

- Roles & responsibilities
- Strategic plan
- Senior mangement support
- Segregation of duties

TRAINING, EDUCATION & AWARENESS

Includes:

- Awareness program
- Scope/coverage
- Methods
- Cyber skills training

DATA PROTECTION

Includes:

- Policies & privacy notices
- PII data mapping
- DPIA & Risk
- Processes for individuals rights

SECURITY RISK MGT

Includes:

- Ownership & support
- Risk management policy
- Risk process
- Risk reporting

SECURITY POLICIES

Includes:

- Policy contents
- Distribution
- Document framework
- Approval/Review

NETWORK SECURITY

Includes:

- Architecture
- Traffic filtering
- Capacity management
- Data in transit

IT SECURITY

Includes:

- Asset management
- Access control
- Vuln management
- Endpoint protection

PHYSICAL SECURITY

Includes:

- Premises perimeter
- Secure office
- Visitors
- Data centre

HR SECURITY

Includes:

- Pre-employment checks
- Contracts
- J ML
- Performance management

SECURITY INCIDENT RESPONSE

Includes:

- Response plan
- Testing
- Skills / knowledge
- Reporting processes

BUSINESS CONTINUITY MGT

Includes:

- BIAs
- BC plan
- DR plan
- Data backups

PROJECT MANAGEMENT

Includes:

- PMO processes
- Change management
- SDLC processes
- Integration

SECURITY EVENT MONITORING

Includes:

- Protective monitoring tools
- Scope (systems)
- Scope (use cases)
- Protection of log data

SUPPLIER ASSURANCE

Includes:

- Risk assessments
- Due diligence
- Contracts / SLAs
- Review

COMPLIANCE, AUDIT & PEN TESTING

Includes:

- Internal Audit
- Management reviews
- Pen testing
- Regulatory/legal

Why other organisations choose PGI

We believe that cyber and information security doesn't need to be overly complicated or vastly expensive.

A tailored approach

Not every business is the same, so we don't approach our projects in the same way. We get to know your organisation and provide appropriate, tailored advice.

Practical and affordable

Solutions are affordable because they are proportionate only to your needs, not a blanket approach.

Cross-sector experience

Our team consists of personnel with backgrounds in security, law enforcement, the military and academia. We've implemented information security measures across a wide range of industries.

Global experience

We have worked with companies in more than 50 countries.

Vendor-neutral advice

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

Other PGI services

Since 2013, we have been helping organisations of all sizes achieve compliance using 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 information security.

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.