

Government Security Profession Career Framework (GSPCF) Rate Card

PGI adopts the Government Digital and Data Profession Capability Framework to price all cyber security roles, ensuring clients receive the right expertise at a clearly defined and consistent level.

Pricing for **Cyber Essentials** and **Cyber Essentials Plus** services are available in the following slides.

GDDPCF Role Level	GDDPCF Rates
Principal / Head of	£1,450-£1,850
Lead	£1,198
Senior	£1,032
Practitioner	£886
Associate	£564
Junior / Assistant	£564
Trainee / Entry / Apprentice	£529

- All prices are exclusive of VAT.
- Our working week: Monday to Friday, 0900 to 1730 GMT (excluding national holidays).
- Any work carried out between 1730 and 0900 on a business day will be charged at 1.5 times the amount shown on the rate card.
- Travel and subsistence are excluded from the rate card and will be charged at cost.
- The rate card includes dedicated project management support.
- Industry standard insurances included in the rate card.

Contact Details

Phone: +44 20 4566 6600
 Email: sales@pgitl.com
 Website: www.pgitl.com

Cyber Essentials Basic pricing



Company size	Bronze	Silver	Gold
 Micro (1-9 employees)	£320	£475	£570
 Small (10-49 employees)	£440	£590	£700
 Medium (50-249 employees)	£500	£650	£780
 Large (250+ employees)	£600	£765	£900

Bronze CE Basic

A cost-effective option for clients who are confident in completing and passing Cyber Essentials Basic without any further support.

Includes:

- Initial marking of the assessment
- **One included resubmission** in the event of a 'More Information Required' result (within five business days)
- If a 'Fail' grade is issued, a new submission will be required and charged separately
- Cyber Essentials handbook

Silver CE Basic

For clients who would like additional support from our assessor and an opportunity to resubmit their assessment if a 'Fail' grade is issued.

Includes:

- **One hour of consultancy support**
- Initial marking of the assessment
- **Two included resubmissions**
 - In the event of a 'Fail' result (within five business days)
 - in the event of a 'More Information Required' result (within five business days)
- Discounted rate for additional resubmissions
- Cyber Essentials handbook

Gold CE Basic

For clients who are seeking additional guidance and support, and more flexibility in addressing assessment feedback.

Includes:

- **Two hours of consultancy support**
- Initial assessment marking
- **Two included resubmissions** in the event of a 'More Information Required' result (within five business days)
- **One included resubmission** in the event of a 'Fail' result (within the 10-day remediation window)
- Discounted rate for additional resubmissions
- Cyber Essentials handbook

Cyber Essentials Plus pricing



Please note: To achieve Plus you will require a valid Basic certificate passed within the last 90 days.

Company size	Bronze	Silver	Gold	Platinum
 Micro (1-9 employees)	£1,582	£1,960	£2,338	£6,500
 Small (10-49 employees)	£1,960	£2,338	£2,717	£8,300
 Medium (50-249 employees)	£2,338	£2,717	£3,095	£10,900
 Large (250+ employees)	£2,717	£3,095	£3,473	£11,500

Cyber Essentials Plus core technical assessments (Included in all CE+ packages)	Description
Pre-engagement consultation	To ensure you're fully prepared ahead of the assessment
Full CE+ Technical Assessment	Conducted by a certified assessor as per NCSC requirements
External interface vulnerability scan (TCP/UDP)	Identifies vulnerabilities on external-facing network infrastructure
Patch management review	Confirms patch levels on sample servers and desktops
Browser & antivirus review	Assesses security configurations on sample devices
Email security assessment	Evaluates email solution's ability to filter malicious content
Mobile device security check	Review of smartphone/tablet security and configuration
Cloud services MFA check	Verifies MFA for all admin and user accounts on cloud platforms

PGI's G-Cloud Service Catalogue



Cyber Security

Penetration Testing

- Generative AI chat penetration testing
- Active Directory
- Build & configuration review
- Cloud review
- External infrastructure
- Internal infrastructure
- Web applications
- Wireless networks
- Intelligence Led

Digital Forensics

Incident Response Management

Phishing Assessments

Cyber Maturity Assessment

IT Health Check

Cyber Essentials Basic & Plus

Cyber Advisor Services

CISO as a Service

Cyber Security Awareness Training

Data Protection Services

Cyber Assurance as a Service

Incident Preparedness

Social Engineering

Physical technical security assessments

AI risk management

Compliance and safety

Cyber incident exercising

PCI DSS

NIST CSF Consultancy

NIS2 Support

GDPR and DPA consultancy

ISO 27001

Business Continuity management (ISO 22301)

DORA

Scoping Process

Every engagement begins with a collaborative scoping conversation to ensure we fully understand your objectives, environment, and any constraints. We'll explore the outcomes you need to achieve, the scale and complexity of the work, and the level of specialist support required.

Pricing is based on the duration and expertise needed to deliver the agreed outcomes. We can provide this as a fixed price or on a time-and-materials basis, depending on what works best for you.

Project timescales are confirmed once the scope is agreed and will reflect the specific requirements and complexity of the engagement. Throughout this process, PGI will work closely with you to shape the right delivery team and approach.

Following scoping, we will provide a clear Scope of Work, outlining the requirements, deliverables, timelines and commercial model, giving you full confidence in how the engagement will run from start to finish.



Engagement Process

Prior to project

Once you've confirmed that the project will go ahead, your dedicated Client Success Manager (CSM) and the consultant(s) delivering the work will arrange a pre-engagement call. This will cover:

- Any logistical or access requirements (onsite or remote)
- Any prerequisites we need from you
- A chance for all parties to ask questions and align expectations

Contact details will be shared, and a start date agreed.

Your CSM will also check in the week before delivery begins to confirm final arrangements and ensure everything is ready.

During the Project

Throughout the engagement, your CSM will remain available to support coordination, answer questions, and address any issues that arise.

If the work involves identifying risks, threats, or vulnerabilities that require urgent attention, our consultants will notify your nominated point of contact immediately (onsite where applicable, or by phone followed by email).

Post project

Once delivery is complete, we will provide your agreed outputs and deliverables within five working days. We remain available to walk you through the findings, answer any additional questions, or discuss wider digital resilience considerations.

Where relevant, the consultant will also conduct a debrief with your team to ensure clarity on outcomes and next steps.

Reference clients



Our accreditations and partnerships

PGI

