

G-CLOUD 15 · CLOUD SUPPORT SERVICE

Service Definition

Penetration testing and IASME certification

Incursion Cyber Security is a veteran-founded UK cyber security consultancy and IASME certification body. We provide penetration testing, Cyber Essentials, Cyber Essentials Plus and IASME Cyber Assurance certification to public sector bodies and their suppliers, delivered by named consultants holding UK Cyber Security Council professional titles.



Contents

- 1 About Incursion Cyber Security
- 2 Services at a glance
- 3 Penetration testing
- 4 IASME certification: Cyber Essentials, Cyber Essentials Plus and Cyber Assurance
- 5 How an engagement runs: onboarding to exit
- 6 Service levels and support
- 7 Pricing
- 8 Security, people and assurance
- 9 Constraints and buyer responsibilities
- 10 Ordering, invoicing and contact

Purpose of this document. It describes the services Incursion Cyber Security offers through the G-Cloud 15 framework under the Cloud Support Service lot: what each service is, how it is delivered, the service levels and pricing that apply, how we handle your data and what we need from you. It should be read alongside our G-Cloud pricing document and terms and conditions.



1 About Incursion Cyber Security

Incursion Cyber Security is a veteran-founded UK cyber security consultancy and IASME certification body, providing penetration testing, Cyber Essentials, Cyber Essentials Plus and Cyber Assurance certification. We are a Cyber Scheme Accredited Company, a G-Cloud 15 and JOSCAR supplier, registered in Somerset with consultants working across the UK.

The company was founded in 2022 by Lewis Lockwood, a former British Army Intelligence Analyst and a Chartered Cyber Security Professional, to do penetration testing the way clients are told it is done: scoped by the tester who will do the work, delivered by a named consultant, reported in plain English and priced without an upsell. We are a fully remote business. Our consultants are based in Somerset, Greater London, West Yorkshire and Renfrewshire and work with organisations anywhere in the UK.

How we work

Four commitments apply to every engagement, and they are the reason public sector buyers choose us over larger providers.

Scoped by an active tester

The person who scopes your engagement is a working penetration tester with the skill set the job needs, not a salesperson or account manager. The scope is accurate, the quote is fixed, and nothing is oversold.

First booked, first served

Engagements are delivered in the order they are booked. We do not move a smaller client to make room for a larger one.

No doubling up

A consultant works on one client engagement at a time. Your test gets the whole of their attention for its duration.

Named consultant, start to finish

Your consultant will be introduced at scoping, they will deliver the work, write the report and answers your questions afterwards.

What we hold

- IASME-licensed certification body: Cyber Essentials, Cyber Essentials Plus and IASME Cyber Assurance
- Certified to Cyber Essentials Plus and IASME Cyber Assurance Level 2 (with Quality Principles) ourselves
- The Cyber Scheme Accredited Company (reference TCS_2625)
- Consultants holding UK Cyber Security Council professional titles in Security Testing, with CREST and Cyber Scheme qualifications
- G-Cloud 15 supplier (Cloud Support Service) and JOSCAR registered supplier (10030864)
- Armed Forces Covenant signatory and Defence Employer Recognition Scheme Bronze award holder

Every accreditation above can be verified against the issuing body's public register. Verification links are published at incursion-security.co.uk/accreditations/.



2 Services at a glance

Two families of service are available through this listing. Penetration testing establishes what an attacker could actually reach in your cloud, application and infrastructure estate. IASME certification independently evidences that baseline and governance controls are in place. Most public sector buyers need both, and because our assessors are penetration testers we can scope them in one conversation or two.

Service	What it answers	Typical duration	Output
External Infrastructure Assessment	What can an attacker on the internet reach and exploit?	2-5 days	Report with rated findings, retest
Internal Infrastructure Assessment	How far could an attacker or compromised device get inside the network?	3-10 days	Report with rated findings, retest
Web Application Assessment	Can the application be abused to access your data, people or finances?	3-10 days	Report with rated findings, retest
Cloud Configuration Review	Is the Microsoft 365, Azure, AWS or Google Cloud tenant configured and permissioned safely?	2-5 days	Report with rated findings, retest
Build and Configuration Review	Is a server, workstation or device build hardened to a defined standard?	1-3 days for multiple builds	Report against benchmark
API Assessment	Does the API enforce what the front end appears to?	2-5 days	Report with rated findings, retest
Mobile Application Assessment	Is the iOS or Android app, and the API behind it, secure?	3-8 days	Report with rated findings, retest
Wireless Configuration Review	Can corporate or guest Wi-Fi be used to reach the network?	1-3 days	Report with rated findings, retest
Physical Security Assessment	Can premises be entered and systems reached in person?	2-5 days	Report with rated findings
Cyber Essentials	Are the five NCSC baseline controls in place? (verified self-assessment)	Marked within 1 working day	Certificate, 12 months
Cyber Essentials Plus	Do the five controls actually work? (audited)	1-3 days on site or remote	Certificate, 12 months
IASME Cyber Assurance Level 1	Is information security governed, not just configured? (verified)	Marked within 1 working day	Certificate, 12 months



Service	What it answers	Typical duration	Output
IASME Cyber Assurance Level 2	Can that governance be evidenced to an independent auditor?	1-3 days audit + IASME review up to 14 days	Certificate, 3 years



3 Penetration testing

A penetration test is a controlled, authorised attempt to break into your systems, carried out by a qualified tester so that you find the weaknesses before an attacker does. It is not a vulnerability scan. A scan lists known software flaws; our consultants chain flaws, misconfigurations and design mistakes together the way a real attacker would and tell you what they could actually reach. The output is a report that says what was found, how serious it is, what it would let an attacker do and how to fix it.

Service lines

External Infrastructure Assessment

Everything you expose to the internet: remote access, mail, DNS, VPN, published services and cloud edge. We enumerate, then attempt to exploit, rather than stopping at a scan result. Includes review of SPF, DKIM and DMARC and of any service reachable without authentication.

Internal Infrastructure Assessment

From the position of an attacker with a network connection, a compromised device or a rogue insider: privilege escalation, lateral movement, credential relaying, Active Directory weaknesses, segmentation and the reach of a single compromised host. Delivered on site or remotely.

Web Application Assessment

Authenticated testing across every user role against the OWASP Top 10 2025 and beyond it: access control, business logic, injection, authentication and session handling, supply chain and error handling. Black-, grey- or white-box as the scope requires.

API Assessment

REST, GraphQL and SOAP services, tested on their own or alongside the application that uses them. Focus on authorisation, object-level access, rate limiting and the trust the API places in its clients.

Mobile Application Assessment

iOS and Android applications, with or without source code: local data storage, transport security, platform controls, reverse engineering resistance and the back-end API.

Cloud Configuration Review

Microsoft 365, Azure, AWS and Google Cloud: identity and conditional access, privileged roles, storage exposure, network controls, logging and the configuration drift that causes most cloud incidents. Read-only credentials are sufficient.

Build and Configuration Review

Windows, Unix and macOS servers and endpoints, and network devices, reviewed against CIS benchmarks or your own standard. Catches misconfiguration before it becomes exploitable.

Wireless Configuration Review



Corporate, guest and rogue Wi-Fi: authentication, segregation from the corporate network, and what a device on the wireless network can reach.

Physical Security Assessment

Overt reviews or covert attempts to enter premises and reach systems, agreed and authorised in advance.

What you receive

One report per engagement, delivered within five working days of the end of testing as standard (ten working days at most for extensive multi-phase programmes). It contains an executive summary in plain English written for a board or senior responsible owner, a technical summary, a scope and coverage statement, and for every finding the observation, its impact, the affected hosts, the remediation and references. Critical and high-risk findings are verified and reported to you immediately during testing rather than held back for the report.

A full worked example against a fictional organisation, with one finding at each severity and retest states shown, is published without registration at incursion-security.co.uk/sample-report/.

Retesting

One day of retesting is included free for every five days of consultancy, to be taken within 90 days of report delivery. Retesting confirms each finding as Remediated, Partially Remediated or Still Open, and checks that fixes have not introduced new issues. Findings marked fixed without a retest are assertions; retested findings are evidence you can put in front of an auditor or regulator.



4 IASME certification

Incursion Cyber Security is licensed by IASME to assess and certify Cyber Essentials, Cyber Essentials Plus and IASME Cyber Assurance. We are the certification body, not a preparation service: we run the assessment and issue the certificate, and our listing can be checked in the IASME certification body directory. Our assessors are penetration testers holding UK Cyber Security Council professional titles.

Certification and testing together. Cyber Essentials Plus checks that five baseline controls work on sampled devices. A penetration test finds the routes an attacker would actually use, including through applications, cloud identity and internal networks that Plus does not examine. Because our assessors are testers, both are scoped in one conversation, sequenced so fixes count towards both, and delivered by one team.

Cyber Essentials

The UK government's baseline certification, owned by the NCSC and delivered by IASME. A verified self-assessment against five technical controls: firewalls, secure configuration, security update management, user access control and malware protection, applied to every device and cloud service in scope. A named assessor marks the submission, returning a result within one working day; if it falls short you have an option to correct the failure and resubmit at no charge. Certificates are valid for twelve months. Current requirements: version 3.3 (Danzell), in force since 27 April 2026.

Cyber Essentials Plus

The same five controls, audited. Within 90 days of the basic certificate an assessor examines a random sample of user devices, every internet gateway and every externally reachable server; runs external and authenticated internal vulnerability scans; tests malware protection by email and browser download; and checks patching within 14 days, separate administrator accounts and multi-factor authentication on cloud services. Assessments are normally remote via screen-share.

IASME Cyber Assurance

For organisations that hold Cyber Essentials and need to evidence governance, risk management, people, physical security, backup, resilience and UK GDPR compliance as well as technical controls, across fourteen themes. Level 1 is a verified self-assessment, valid for twelve months. Level 2 is an independent audit (document review, staff interviews, observation), moderated by IASME and valid for three years provided Level 1 and Cyber Essentials are kept current. Many sectors accept audited Level 2 as an alternative to ISO 27001 for smaller organisations.



5 How an engagement runs

Onboarding

- 1. Enquiry and scoping call.** Free of charge. For penetration testing, an active tester with the relevant skill set agrees what is in and out of scope, the testing approach (black-, grey- or white-box), the environments, windows and constraints, and what the test is for. For certification, we confirm organisation size and send a short standard question set, reviewed by an assessor; a call is offered if anything is unclear.
- 2. Fixed-price proposal.** Issued within two working days of scoping, stating scope, days, price, and potential dates. The price does not change unless the scope does.
- 3. Authorisation and rules of engagement.** Written authorisation from the system owner, contacts and escalation routes, exclusions, testing windows, and what happens if a critical issue is found, confirmed before anything starts.
- 4. Kick-off.** A short call with the named consultant to confirm access, accounts, test data, on-site arrangements where relevant and the reporting contact.
- 5. Delivery.** By the consultant introduced during scoping, on the agreed dates. Critical and high findings are verified and notified immediately. Progress is reported at agreed intervals on longer engagements.
- 6. Report and debrief.** Report within five working days of the end of testing. A debrief call is included on request for no additional charge, with the consultant walking your technical and non-technical stakeholders through the findings and priorities.
- 7. Retest.** Booked at your convenience within 90 days of the report; one day per five days of testing at no charge, further days at the day rate. Additional retesting available at standard day rate.

Offboarding and exit

There is no lock-in. Engagements are fixed-scope and end on delivery of the report and any retest. On completion, or on termination, we remove any access, accounts, devices or credentials provided to us. Reports and supporting evidence are yours; we retain an encrypted copy for twelve months to support the retest window and any queries, then delete it, or delete earlier on your written request and confirm deletion. No data is held that would prevent you moving to another supplier.

Data handling

Engagement data, findings and reports are stored on UK-hosted, encrypted systems with access restricted to the consultants working on your engagement. Client data taken from systems during testing is limited to what is necessary to evidence a finding, is redacted in the report where sensitive, and is subject to the same retention and deletion terms. We hold Cyber Essentials Plus and IASME Cyber Assurance Level 2 ourselves, and our information handling is assessed annually as part of maintaining them.



6 Service levels and support

Measure	Commitment
Scoping call	Free; offered within two working days of enquiry
Proposal	Fixed price, within two working days of scoping call
Critical and high-risk findings	Verified and notified to your nominated contact immediately during testing, by phone and in writing
Report delivery	Within five working days of the end of testing as standard; ten working days maximum for extensive multi-phase programmes
Retest	One day per five days of testing included; within 90 days of report delivery
Cyber Essentials and Cyber Assurance Level 1 marking	Assessors return results within one working day of submission
Cyber Essentials Plus scheduling	Booked inside the 90-day window following the basic certificate; planned with you at the outset
Support hours	09:00-17:30, Monday to Friday, excluding English bank holidays; out-of-hours testing windows by arrangement
Support route	Named consultant with a direct telephone number and email for the life of the engagement
Response to queries	Acknowledged within one working day; answered by the consultant who did the work, not a help desk
Service constraints	Testing windows, exclusions and rate limits agreed at scoping; no disruptive techniques without your explicit agreement

If we miss a commitment

If a retest cannot be delivered within the 90-day window for reasons within our control, the window is extended at no charge. Any dispute is handled first by the engagement lead and then by a director, with a written response within five working days.

Outages and business continuity

Our services are consultancy delivered by people rather than a hosted platform, so there are no maintenance windows or platform availability figures to report. Delivery continuity is protected by the named consultant model backed by a second consultant briefed on every engagement, and by the supervision structure described in section 8. If a consultant becomes unavailable, you are told the same day and offered either a rescheduled date or a briefed replacement.



7 Security, people and assurance

Who does the work

Every engagement is scoped and delivered by a named consultant holding an appropriate qualification or professional title (issued by the UK Cyber Security Council in the Security Testing specialism), or working under the direct supervision of one. Our consultants also hold CREST and Cyber Scheme qualifications.

Vetting and clearance

Where an engagement requires vetting, consultants hold SC clearance as a minimum. Where it does not, consultants hold a DBS check as a minimum.

Our own assurance

We hold Cyber Essentials Plus and IASME Cyber Assurance Level 2 with Quality Principles, are a Cyber Scheme Accredited Company, and are a JOSCAR registered supplier. We carry professional indemnity and public liability insurance; certificates and cover levels are available on request and are included in our G-Cloud supplier documentation. We are a signatory to the Armed Forces Covenant and hold the Defence Employer Recognition Scheme Bronze award.

Information security during engagements

- Testing is conducted from dedicated, hardened consultant systems with full-disk encryption; test devices supplied to facilitate internal engagements are wiped on completion.
- Credentials and access provided to us are used only for the agreed scope, stored in an encrypted vault for the engagement, and removed and confirmed removed at exit.
- Evidence gathered is the minimum needed to demonstrate a finding, redacted in the report where sensitive, and held under the retention terms in section 5.
- Any security incident affecting client data is notified to the client within 24 hours of our becoming aware.

Standards and methodology

Testing follows a documented methodology aligned to the OWASP Testing Guide and Top 10 (2025), the Penetration Testing Execution Standard, CIS benchmarks and NCSC guidance. Findings are rated by real-world impact, not scanner score.



8 Constraints and buyer responsibilities

Technical requirements

Penetration testing requires no software to be installed on your estate. For external testing we need the in-scope addresses and hostnames and confirmation of ownership. For internal testing we need either a network connection for a consultant on site or a supplied test device connected to the network. For application and API testing we need test accounts for each user role and a non-production environment where one exists. For cloud reviews we need read-only credentials to the tenant or subscription. For Cyber Essentials Plus, a vulnerability scanning agent may need deploying to a sample of devices, we will also need a members of your team available for a screen-sharing session.

What we need from you

- Written authorisation from the owner of every system in scope before testing begins, including third-party hosting providers where their terms require notice.
- A nominated technical contact available during testing windows, and an escalation contact for critical findings.
- Accurate scope information at the scoping stage; changes after the proposal are agreed as scope changes and may affect dates and price.
- Backups of in-scope systems before testing. Testing avoids disruptive techniques unless agreed, but any live system carries some risk.
- For certification, truthful and complete answers to the question set, and timely access to sampled devices for Plus.

Constraints

- Services are delivered UK-wide; international delivery is by arrangement.
- We do not offer incident response; where an engagement uncovers an active compromise we tell you immediately and can refer you to a partner.
- Certification scope declarations must meet IASME requirements; a certificate covering a subset of the organisation states that it does.
- Testing of systems handling UK government information at OFFICIAL and above under the NCSC CHECK scheme is outside the scope of this listing.



9 Ordering, invoicing and contact

Ordering through G-Cloud

Identify the service on the Digital Marketplace, contact us for a free scoping call, and we issue a fixed-price proposal against the G-Cloud call-off terms. On acceptance you raise a purchase order or call-off contract referencing this framework, and dates are booked in the order received. Buyers may also run a further competition where their procurement rules require it; we respond within the stated timescale.

Invoicing

Invoices are issued on delivery of the report or access to the IASME self-assessment portal, payable within 30 days by BACS. We can invoice per phase for multi-phase programmes and support purchase-order and e-invoicing requirements.

Termination

Either party may terminate a call-off on written notice. Work delivered to the date of termination is invoiced at the day rate; scheduled days fall under the cancellation scale in section 7. On termination we remove all access provided to us, return or delete your data on request and confirm both in writing.

Trial

We do not offer a trial service; scoping calls are free and a sample report is published without registration at incursion-security.co.uk/sample-report/ so that buyers can see exactly what they will receive before committing.

Contact

Company	Incursion Cyber Security Ltd
Registered office	1 Bushy Coombe, Midsomer Norton, BA3 2RW
Company number	14303576 (England and Wales)
VAT number	429058190
Telephone	+44 7496 256 424
Email	info@incursion-security.co.uk
Website	incursion-security.co.uk
Framework	G-Cloud 15, Cloud Support Service
Document version	2.0, September 2026