SERVICE DEFINITION DOCUMENT
FRAMEWORK MATURITY ASSESSMENT

Our address
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

Give us a call
0333 939 8080

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

About JUMPSEC

JUMPSEC is a UK-based cyber security consultancy, established in 2012, with a proven track record in offensive testing, incident response, managed detection, and advisory services for both public and private sector organisations. Our work is led by skilled professionals with extensive experience in red teaming, security engineering, and incident response, ensuring that our services are rooted in real-world knowledge and practical expertise.

We place a premium on assurance. Our teams include CHECK and CREST-qualified penetration testers, as well as NCSC CIR-approved incident responders and NCSC CIE-accredited Incident Managers, enabling us to deliver a wide range of government-level security engagements. We have deep experience deploying and managing Microsoft security technologies such as Microsoft Defender and Sentinel, particularly within regulated environments. Our approaches and documentation are consistent with recognised standards including the NIST Cyber Security Framework, CIS Controls and CAF, and our reporting is clear and purposeful, catering to both technical specialists and executive decision-makers.

Clients use JUMPSEC to achieve three outcomes:

- to reduce the risk of significant security incidents
- to speed up the detection and containment of threats, and
- to demonstrate robust governance to stakeholders such as boards, auditors, and insurers

Our services are transparent and collaborative—clients are given clear scopes, well-defined engagement terms, daily updates during testing, and strong evidence to support their security posture. We prioritise remediation advice based on business impact, not just automated scan results.

Protecting client data is at the heart of our operations. JUMPSEC acts as a data processor under UK GDPR and DPA, adheres to principle-of-least-privilege access, and only retains evidence for periods agreed with clients. Where necessary, our personnel hold BPSS or SC clearance, and we can provide reports and artefacts in accessible formats to meet WCAG 2.1 AA standards.

Our public sector experience covers central and local government, healthcare, education, and critical national infrastructure. In the private sector, we support clients in finance, manufacturing, logistics, and technology. We often deliver projects alongside complementary services, such as red and purple teaming, detection engineering, and incident response retainers, to drive measurable improvements and tangible returns.

We continually refine our services to address the evolving needs of our clients, frequently developing tailored solutions to unique challenges. Our approach is adaptable and shaped by each client's specific situation, so the best way to understand how we can help is to discuss your needs directly with us before RFP release.

This overview outlines JUMPSEC's broad capabilities and demonstrates how our expertise can be applied to deliver practical, threat-focused security for your organisation. To find out more about how we can address your cyber security requirements, please get in touch for a straightforward conversation.

Example use cases

Local authority — CAF maturity snapshot for Audit & Governance

JUMPSEC delivered a CAF maturity snapshot for a unitary authority ahead of committee scrutiny. We defined the scope to cover Detect and Respond outcomes, conducted interviews with ICT, Legal, and Procurement teams, and carried out light technical sampling for logging and backup controls. The scorecard highlighted where event fidelity was weak and isolation thresholds were unclear. We provided a gap register with acceptance tests that internal audit could reuse at the next checkpoint.

NHS provider — ISO 27001 surveillance readiness check

A trust asked us to assess its current ISMS scope ahead of surveillance. We at JUMPSEC reviewed evidence and conducted interviews, uncovering incomplete risk treatment and limited internal audit sampling. We clarified what needed closure and how to demonstrate it through our scorecard and gap register. The pack we delivered enabled a focused pre-audit clean-up without the need to expand documentation.

Central government agency — NIST CSF 2.0 baseline

A department asked JUMPSEC for a NIST baseline to guide spending decisions. We sampled controls and confirmed strengths in identity governance, but identified gaps in detection analytics and recovery testing. We produced a scorecard and heatmap that directed investment discussions, and our acceptance criteria enabled an independent verifier to confirm progress in the following quarter.

National charity — CIS Controls quick look

A charity asked us for a concise CIS v8 snapshot to support insurer engagement. We at JUMPSEC reviewed the evidence and found that device hardening was inconsistent and log coverage was limited. We assessed the organisation and delivered a pragmatic maturity score, along with a small set of closure tests focused on controls designed to reduce fraud and mailbox compromise risks.

Service Overview

JUMPSEC delivers an evidence-led assessment against a chosen framework (ISO/IEC 27001/27002, NIST CSF 2.0, CIS Controls v8, or NCSC CAF). We determine current maturity, highlight control gaps, and provide a defensible scorecard with clear, testable acceptance criteria for uplift. The scope is assessment-only: no implementation, no policy drafting, and no remediation delivery.

Objectives

- Establish (or assess against a pre-existing) a baseline maturity level against the selected framework.
- Identify control gaps with mapped risk and audit impact.
- Provide concise, testable acceptance criteria to confirm closure.
- Equip boards, SIROs, auditors, and insurers with a defensible snapshot.

Approach

JUMPSEC runs a structured review of policies, processes, and representative technical controls. We interview control owners, sample evidence, and verify effectiveness where feasible. Findings are normalised to the framework's structure and presented as a scorecard, gap register, and acceptance tests that third parties can verify.

Method

- **Plan:** Confirm framework, scope boundary, entities, evidence handling, and stakeholders..
- **Discover:** Collect existing policies, registers, diagrams, contracts, and previous audits; interview control owners.
- **Validate:** Sample technical controls (identity, endpoint, backup, logging, cloud) non-destructively to confirm effectiveness.
- **Analyse:** Score maturity per clause/control/subcategory/outcome; map risks; define acceptance criteria for closure.
- **Debrief:** Present scorecard, gap register, and a prioritised heatmap; agree next measurement cadence.

Deliverables

- **Maturity Scorecard** aligned to ISO/NIST/CIS/CAF with level definitions and rationale.
- **Control Gap Register** with evidence references, risk notes, owners, due dates, and acceptance criteria.
- **Assurance Pack:** summary for boards and audit, heatmap by domain, and sample test scripts for internal verification.
- **Traceability:** explicit mappings (e.g., ISO Annex A controls, NIST CSF categories, CIS Safeguards, CAF outcomes) embedded in the artefacts.

(Standards and alignment are integrated into these deliverables, not listed separately.)

Outcomes and benefits

- Clear, defendable view of current maturity and where it falls short.
- Precise closure tests that reduce debate during audits and attestations.
- Faster planning for remediation and budget setting (outside this scope).
- Improved insurer and regulator confidence

Pricing model

Fixed price per assessment scope (single framework, single entity), or time-and-materials for multi-entity or multi-framework baselines. Pricing factors include number of entities, evidence volume, technical sampling depth, and interview count.

Typical Timelines

- Planning and evidence request: 3–5 working days.
- Assessment and analysis: 5–15 working days (scope-dependent).
- Report issue: 5–10 working days after testing completion.

Security and assurance

Facilitation is delivered by experienced practitioners using peer-reviewed methods and internal quality checks. Materials are reproducible and traceable to session evidence.

Team and roles

- **Engagement Lead.** Scope, governance, quality management, and stakeholder alignment.
- **Framework Assessor(s) (ISO/NIST/CIS/CAF etc).** Evidence review, interviews, scoring, and analysis.

- **Coordinator.** Artefacts, scheduling and audit logistics

Buyer responsibilities

- Nominate an executive sponsor, control owners.
- Provide requested artefacts and facilitate interviews.
- Confirm scope boundaries and any legal or contractual constraints.

JUMPSEC responsibilities

- Conduct an evidence-led, non-disruptive assessment.
- Protect confidentiality and handle artefacts under least-privilege access.
- Produce clear, auditable outputs with acceptance criteria.

Data protection and privacy

The buyer remains data controller. Evidence is transferred securely, stored with access logging, retained only as agreed, and returned or destroyed at close.

Constraints and assumptions

- Assessment-only engagement: no remediation, policy creation, or control operation.
- Third-party environments require consent for evidence access.
- No destructive testing; technical sampling is read-only. No destructive testing; any technical sampling is non-disruptive.
- Personnel with BPSS/SC clearance are available where required.
- Reports can be supplied in accessible formats on request (WCAG 2.1 AA)

Related services

- Framework Advisory and Consultancy (implementation planning)
- vCISO
- Executive and Board Cyber Briefing / Board Coaching
- IR Readiness Review / Breach Readiness Review
- Log Validity Assessment

Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

0333 939 8080

hello@jumpsec.com

www.jumpsec.com