SERVICE DEFINITION DOCUMENT
FRAMEWORK ADVISORY AND CONSULTANCY

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 baseline and improvement plan

JUMPSEC worked with a unitary authority to deliver a defensible view against the NCSC CAF. We sampled identity, backup, logging, and supplier controls, and interviewed owners from ICT, Legal, and Procurement. We framed the gaps we found in terms of service impact and regulator expectations. JUMPSEC sequenced privileged access uplift, immutable backups, and log validity fixes within a clear plan, and we scheduled quarterly checks. Leadership used the CAF scorecard we provided to brief the Audit & Governance Committee and track progress.

NHS provider — ISO 27001 certification readiness

JUMPSEC supported a trust seeking certification across a defined ISMS scope. We reviewed evidence and identified policy gaps, incomplete risk treatment, and limited internal audit coverage. Together, we completed a pragmatic set of policies, clarified SoA justifications, and introduced a lightweight audit programme with sampling scripts. Stage 1 went ahead with only minor observations, and we closed Stage 2 after delivering targeted technical fixes and updating supplier clauses.

Central government agency — NIST CSF 2.0 target profile

A department asked us for a NIST target profile that matched their risk appetite and addressed legacy estate constraints. We ran workshops to set priorities, and JUMPSEC carried out technical sampling to validate identity, detection, and recovery capabilities. We then linked subcategories to investment options and measurable KPIs. JUMPSEC supported quarterly governance, tracking progress against the target profile and guiding spending decisions.

Manufacturer — CIS Controls uplift across plants

JUMPSEC worked with a global manufacturer to establish a controls baseline suitable for mixed Windows, Linux, and OT-adjacent networks. We sampled environments and identified inconsistent hardening, weak logging fidelity, and excessive supplier access. Together, we applied CIS Safeguards by tier, rolled out baselines with acceptance tests, and set a straightforward internal audit schedule. Our KPIs demonstrated improved coverage and quicker investigations, all without disrupting production.

Service Overview

JUMPSEC helps organisations assess, achieve, and sustain compliance and maturity against leading governance frameworks including ISO/IEC 27001/27002, NIST CSF 2.0, CIS Controls v8, and the NCSC Cyber Assessment Framework (CAF). We baseline your current posture, map controls to business risk, and build a practical improvement plan with measurable outcomes. We translate framework language into clear actions for technology, data, suppliers, and operations, then verify uplift through evidence, metrics, and internal audit cycles.

Objectives

- Establish a defensible baseline against target frameworks and obligations.
- Prioritise control improvements that reduce real risk and audit exposure.
- Produce clear artefacts for boards, accreditors, regulators, and insurers.
- Embed a repeatable measurement and internal audit cadence.

Approach

We start with a short discovery to confirm scope (frameworks, entities, systems), drivers (regulatory, contractual, audit), and risk appetite. JUMPSEC runs a control evidence review, interviews control owners, and samples technical configurations. Gaps map to risks, not just clauses. We define a target state, deliver a sequenced improvement plan, and set acceptance criteria. Where certification or formal assessment is in scope, we prepare you for Stage 1/2 audits or independent reviews and support issue closure with evidence.

Method

- **Plan:** Agree target frameworks, entities, and boundaries; confirm evidence handling and governance.
- **Discover:** Collect policies, asset/data flows, technical baselines, supplier contracts, and existing audits; interview owners.
- **Validate:** Sample technical controls (identity, endpoint, logging, backup, cloud) and test a subset to confirm effectiveness.
- **Analyse:** Map findings to ISO/NIST/CIS/CAF outcomes; define risk treatment, owners, acceptance criteria, and KPIs.
- **Debrief:** Present the improvement plan, Statement of Applicability (ISO), target profile (NIST), or CAF scorecard; agree cadence and internal audit plan.

Deliverables

- **Executive briefing t**hat links framework gaps to business and audit risk.
- **Baseline Assessment Pack:** clause/control-by-control results, evidence references, and maturity.
- **Improvement Roadmap:** prioritised actions, owners, milestones, acceptance, and quick wins.
- **Risk Treatment Register** aligned to the chosen framework (e.g., ISO Annex A control mapping, NIST CSF categories/subcategories, CIS Safeguards).
- **Policy & Procedure Set** (create or refine): information security policy suite, supplier security, incident management, business continuity/DR, data protection overlays.
- **Statement of Applicability** (ISO only) and **Audit Readiness Pack** (Stage 1/Stage 2 or independent review).
- **Measurement & Internal Audit Programme:** KPIs/KRIs, sample test scripts, audit schedule, and evidence templates.
- **Assurance Artefacts** for boards, SIROs, and regulators: CAF outcome sheets, conformance letters, and progress dashboards.

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

Outcomes and benefits

- Clear route to certification or attestation with fewer audit surprises.
- Control improvements that cut real attack paths, not just paperwork.
- Repeatable governance with metrics that decision-makers trust.
- Stronger insurer, regulator, and customer confidence.

Pricing model

Fixed price for a defined scope (single framework or crosswalk), or time-and-materials for complex, multi-entity programmes. Pricing Drivers include entity count, system breadth, supplier landscape, depth of technical sampling, and audit support.

Typical Timelines

- Planning and discovery: 5–10 working days.
- Assessment and analysis: 10–20 working days (scope-dependent).
- Report issue: 5–10 working days after testing completion.
- Audit preparation, remediation support, and re-test: by agreement.

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. Where appropriate, observed behaviours are mapped to MITRE ATT&CK and translated into detection opportunities for SOC/EDR teams. Accessibility options are available on request.

Team and roles

- **Engagement Lead.** Scope, governance, quality management, and stakeholder alignment.
- **Framework Lead (ISO/NIST/CIS/CAF etc).** Assessments, mappings, and audit readiness.
- **Technical Assessor(s).** control sampling and evidence validation.
- **Coordinator.** Artefacts, interviews, and audit logistics

Buyer responsibilities

- Nominate an executive sponsor, control owners, and audit liaison.
- Provide access to policies, system owners, and technical evidence.
- Align change control and budget to adopt improvements.

JUMPSEC responsibilities

- Nominate an executive sponsor, control owners, and audit liaison.
- Provide access to policies, system owners, and technical evidence.
- Align change control and budget to adopt improvements.

Data protection and privacy

The buyer is the data controller, with JUMPSEC as processor. Only essential evidence is collected and kept, following secure transfer, access controls, and set retention periods. After the engagement, data and credentials are returned or destroyed. Final deliverables include an action log, debrief materials, and an evidence-retention statement.

Constraints and assumptions

- No destructive testing; any technical sampling is non-disruptive.
- Third-party environments require consent for evidence access.
- Third-party involvement requires prior written consent.
- Personnel with BPSS/SC clearance are available where required.
- Reports can be supplied in accessible formats on request (WCAG 2.1 AA)

Related services

- 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