SERVICE DEFINITION
BUSINESS CONTINUITY PLANNING

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 — citizen-service continuity during data-centre outage

A unitary authority identifies revenue and benefits, adult social care, and customer contact as priority services. Workshops reveal dependence on a single colocation facility and shared identity services with a regional partner. Decision thresholds for isolating shared identity are unclear and supplier cut-over steps lack owner attribution. The programme establishes explicit isolation and re-route criteria, creates site-agnostic identity access for priority roles, and documents a supplier call-off for emergency hosting. A rehearsal walks leadership through activation, supplier engagement, and citizen-facing communications. Post-exercise actions tighten call-trees, update scripts for vulnerable-citizen communications, and confirm change windows for identity failover. Service owners report faster decision-making and fewer hand-off delays.

Water utility (CNI) — treatment continuity during OT network isolation

A UK water company models loss of the corporate-OT link after suspicious activity appears in shared services. Operations need safe isolation without breaching water quality or abstraction limits. Workshops map dependencies between telemetry, dosing control, lab results, and regulatory sampling. The plan separates essential telemetry from corporate identity, defines a brokered operations channel, and issues pre-approved dosing set-points with witnessed dual control. A rehearsal walks shift leads through isolation of the interconnect, activation of offline procedures, and timed sampling with manual logging. Actions tighten call-trees with the DWI and Environment Agency, cache supplier firmware packs at sites, and add a return-to-normal checklist that confirms trend stability before reconnecting. The operator reports faster isolation decisions and no breach of statutory reporting during the drill window.

Telecoms network operator (CNI) — mobile core service continuity under signalling flood

A national telecoms provider tests continuity when signalling storms degrade mobility management and customer authentication. Impact analysis ranks emergency services routing, lawful intercept compliance, and priority enterprise APNs above consumer throughput. The plan defines traffic shedding rules, priority profiles, and a cross-domain command structure joining NOC, security, and regulatory liaison. A live-play exercise simulates regional overload and triggers stepwise activation: throttle non-critical APNs, pin priority devices to reserved capacity, and switch care channels to status-first scripts. Evidence from the drill confirms stable E112 routing, preserved enterprise SLA paths, and timely regulatory updates. Post-exercise actions formalise a crisis cadence with the Home Office, add automated dashboards for priority KPIs, and pre-stage configuration bundles for rapid rollback once signalling recovers

Service Overview

JUMPSEC designs and refreshes Business Continuity Plans that work under pressure. We join cyber disruption, supplier dependency, and operational recovery into clear, executable run-books. We focus on critical services, people, premises, technology, and third parties. Outputs turn impact analysis into decisive actions with roles, decision thresholds, and tested workarounds aligned to crisis management and incident response.

Objectives

- Establish a current, risk-based continuity baseline for critical services.
- Define decision points, authorities, and credible workarounds for outages.
- Map supplier and technology dependencies to recovery priorities and constraints.
- Produce tested, owner-attributed run-books with measurable acceptance criteria.

Approach

We start with a short planning session to agree scope, governance, and evidence handling. We run business impact analysis to understand tolerances and interdependencies. We map suppliers, shared platforms, data flows, and sites. We design recovery strategies that reflect real-world constraints and regulatory obligations. We embed triggers, escalation paths, and communications steps. We prove the design through exercises and land changes through change control with defined rollback points

Method

- Plan — confirm objectives, stakeholders, evidence, and cadence; agree authority and change windows.
- Discover — run BIA workshops; collect service metrics, supplier contracts, RTO/RPOs, and site constraints.
- Validate — stress-test assumptions; model incident timelines; confirm feasibility of workarounds.
- Analyse — select strategies; assign roles, decision thresholds, and external engagement routes; define acceptance tests.
- Debrief — deliver plans, playbooks, contact trees, and exercise schedule; agree ownership and revalidation dates.

Deliverables

- Executive briefing explaining impact scenarios, priority services, and continuity posture.
- Service-level BCP Packs with activation triggers, roles and responsibilities, decision thresholds, communications steps, supplier cut-over, and return-to-normal criteria.

- Dependency Register across people, sites, technology, data flows, and third parties with owners and recovery constraints.
- Contact and Call-Tree bundle for crisis leadership, operations, and suppliers, with rehearsal scripts and verification checks.
- Exercise Plan and artefacts (table-top or live-play), including objectives, scenarios, injects, and evaluation criteria.
- Embedded alignment to ISO 22301, NCSC resilience guidance, and ISO/IEC 27035 where BCP intersects incident response.

Outcomes and benefits

- Faster, more confident decision-making under pressure.
- Clear hand-offs between crisis leadership, operational teams, and suppliers.
- Executable workarounds that preserve priority services during outages.
- Audit-ready artefacts that support governance, regulators, and insurers.

Pricing model

Fixed price per business unit or service family, or time-and-materials for large, multi-entity programmes. Price drivers include number of critical services, supplier complexity, multi-site considerations, and exercise depth.

Timelines

- Planning and access preparation: 3–5 working days.
- Discovery and design: 2–4 weeks elapsed time depending on service count and supplier breadth.
- Report issue: 5–10 working days after testing completion.
- Optional re-test and change assurance: by agreement.

Team and roles

- Engagement Lead for governance, cadence, and quality.
- BCM Specialist(s) for BIA, dependency mapping, and plan design.
- Exercise Director for scenario design, facilitation, and evaluation.
- Coordinator for logistics, artefacts, and document control.

Buyer responsibilities

- Nominate an executive sponsor and service owners for each critical service.
- Provide service metrics, supplier contracts, and site information.
- Align change control and communications approvals for plan adoption and exercises

JUMPSEC responsibilities

- Operate within agreed authority and minimise operational disruption.
- Deliver clear, testable plans with owners, thresholds, and acceptance tests.
- Handle materials securely with least-privilege access, time-boxed retention, and approved destruction or return.

Data protection and privacy

The buyer is data controller; JUMPSEC acts as processor. Only minimum necessary evidence is collected and retained. Secure transfer, strict access control, and agreed retention periods apply. Artefacts are returned or securely destroyed on completion.

Constraints and assumptions

- No destructive testing.
- Third-party participation subject to consent and contract terms.
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Cyber Incident Exercising (NCSC Assured)
- Incident Response Retainers (NCSC CIR)
- Response Playbook Development

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com