



Information Security
Consultancy Services
Specification Document

Table of Contents

<i>Service Overview</i>	<i>2</i>
<i>Onboarding.....</i>	<i>3</i>
<i>Offboarding and exit management</i>	<i>3</i>
<i>Service Levels.....</i>	<i>4</i>
<i>After Sales Support.....</i>	<i>4</i>
<i>Technical Requirements</i>	<i>4</i>
<i>Access to Data.....</i>	<i>5</i>
<i>Security</i>	<i>5</i>

Service Overview

Veliax's Information Security Consultancy Services provide expert support to help organisations strengthen their security posture, reduce cyber risk and meet the expectations of recognised standards, frameworks and regulatory requirements.

Our consultants work collaboratively with organisations to build proportionate, effective and sustainable security capabilities that protect information assets and enable confident, risk-informed decision-making.

The service spans assessment, strategy, governance, operational delivery and advisory support, helping organisations improve security maturity, implement robust controls and embed strong security practices across people, processes and technology.

Services include:

- Information security gap analyses and maturity assessments
- Information security strategy and roadmap development
- Information Security Management System (ISMS) design, implementation, management and ISO 27001 certification support.
- Security policy, standard and framework development
- Risk assessments, threat analysis and supplier security assurance
- Business continuity and incident response planning
- Technical and organisational control evaluation
- NCSC Cyber Assessment Framework implementation and audits
- Penetration testing (OSCE, OSCP)
- Security training, education and awareness activities

Veliax consultants have extensive experience supporting UK public sector organisations and hold advanced information security certifications including ISC2 CISSP, ISO 27001 Lead Implementer/Auditor, and Chartered Information Security Professional.

We provide pragmatic, actionable and proportionate security advice that aligns with organisational objectives and supports robust, measurable security improvement.

Onboarding

Our onboarding process is streamlined, ISO 9001-aligned, and designed to give customers clarity and confidence from the outset.

Understanding requirements and objectives

We begin by taking the time to fully understand your needs, priorities and intended outcomes. This includes reviewing any existing documentation, discussing current challenges and confirming what success should look like.

Developing a tailored proposal

Based on this understanding, we prepare a tailored proposal outlining the services Veliax will provide, the approach we recommend, the expected deliverables and the intended timelines. Work does not begin until you are satisfied that the proposed services meet your requirements.

Accommodating security requirements

We are able to work within your specific information security policies, access controls and tooling. Where additional security measures are required, we integrate them into the engagement from the start.

Project Delivery

Consultant assignment

We allocate consultants with the most relevant expertise to ensure the engagement is delivered effectively. Each assignment is based on sector experience, subject-matter knowledge and the specific requirements of the project. This approach ensures customers receive support from practitioners who are well-matched to their organisation and objectives.

Kick-off and planning

The delivery phase begins with a structured kick-off meeting where we walk through the scope, confirm key stakeholders, roles and responsibilities, and agree a project plan. The plan sets out the phases, milestones and deliverables so all parties have a shared, transparent view of how the engagement will progress.

Ongoing communication

Throughout the engagement, we maintain regular communication to provide updates, discuss emerging findings, and highlight any risks or dependencies. Our aim is to ensure you always know how work is progressing and what is coming next.

Collaborative working

We work closely with your teams and stakeholders, combining our expertise with your organisational knowledge. This collaborative approach ensures recommendations are practical, informed and aligned with your internal ways of working.

Maintaining quality

Progress is monitored against the agreed plan and all deliverables undergo internal quality assurance. If priorities evolve, we adjust the approach in consultation with you to keep the engagement aligned with your objectives.

Where an outsourced Information Security Officer or similar role is provided, we establish role responsibilities, escalation routes, and reporting cycles.

Offboarding and exit management

At the end of an engagement, we ensure a smooth and transparent handover.

Offboarding may include:

- Transfer of all documents, work products, templates and outputs created during the engagement
- Completion of any agreed transition activities
- Handover meeting or presentation summarising key findings, progress and recommendations
- Return or secure deletion of customer data, as required
- Support to transition responsibilities to internal teams or another supplier

Customers retain full access to all deliverables produced for them.

Service Levels

Service levels are designed to support timely advice and reliable delivery.

Response to enquiries

- Queries relating to service delivery or commercial matters receive prompt responses.
- Standard support hours: Monday–Friday, 9am to 5pm (UK time).
- Out-of-hours or extended support can be agreed on an engagement-by-engagement basis.

Delivery approach

- Work is delivered either remotely or on-site, depending on customer requirements.
- Service flexibility ensures alignment with organisational priorities and timelines.
- Regular progress updates and checkpoints are provided throughout the engagement.

After Sales Support

Following completion of an engagement, we offer:

- Follow-up clarification and Q&A support
- Optional ongoing advisory hours
- Check-ins to review progress or implementation of recommendations
- Access to updated templates, guidance and good practice (where agreed)

Where the customer purchases an ongoing subscription or retainer, advisory services continue uninterrupted.

Technical Requirements

As this is a consultancy service, the technical requirements are minimal.

Typical needs include:

- Access to relevant documentation, systems, policies and stakeholders
- Secure communication channels (email, MS Teams, SharePoint, etc.)
- Optional access to internal project or collaboration platforms
- Remote access arrangements where operational work requires it

We adapt to customer IT security requirements and operate within their approved environments.

Access to Data

During an engagement, Veliax may access limited personal data or business information needed to fulfil agreed work. All such information is handled with the utmost care, applying strict confidentiality and data-minimisation practices throughout the engagement.

Upon exit:

- All customer information is securely deleted or returned, depending on contractual requirements
- No customer data is retained unless legally required
- Secure deletion is evidenced upon request

Security

Veliax operates an ISO 27001-aligned information security management system and holds Cyber Essentials and Cyber Essentials Plus certification.

Veliax has implemented proportionate risk-based controls to mitigate its information security risks.

Security measures include:

- Comprehensive Information Security Policies
- Secure configuration of devices and systems
- Consultant awareness and training
- Use of secure communication mechanisms

- Role-based access controls supported by robust joiners, movers and leavers processes
- Background checks and government security vetting for staff.

Where additional security measures are required by our customers, we integrate them into our existing management system.