

PROFESSIONAL PARTNER OFFER

Outsourced Specialist Advisory Services

Specialist AI, data, digital governance, due diligence and operational-risk capability for UK law firms, accountancy practices and professional advisers.

Delivered by Sienda Ltd

London, United Kingdom

www.sienda.co.uk

THE PROPOSITION

Your firm retains the client relationship. Sienda supplies the specialist delivery capability when a matter moves into AI, technology, data, digital risk or organisational transformation.

Each engagement is scoped to the client's circumstances. The service descriptions in this document define the purpose and typical boundaries of the services rather than a fixed checklist.

Prepared for discussion with prospective professional-firm partners. Commercial terms and scope are agreed engagement by engagement.

Sienda ltd

1. The proposition

A specialist delivery capability that professional firms can bring into client engagements without building the capability in-house.

Law firms, accountancy practices and advisory firms increasingly encounter client matters where legal, tax, financial or corporate advice intersects with AI, technology, data, digital governance and operational risk.

Those issues are often commercially material, but they do not always justify recruiting and maintaining a permanent internal specialist team. Sienda provides that specialist layer on a project basis.

We do not seek to displace the instructing firm. The professional firm can remain the primary adviser and relationship owner while Sienda scopes and delivers the specialist workstream.

EXTEND YOUR OFFER	RETAIN THE CLIENT	DELIVER DEEPLY
Add specialist capability without fixed recruitment cost.	Keep the engagement within your professional relationship.	Bring in focused expertise only where the matter requires it.

Who this is for

- Law firms dealing with corporate transactions, commercial contracts, technology, privacy, employment, regulatory matters or disputes where digital evidence and operational realities matter.
- Accountancy and corporate-finance firms supporting acquisitions, disposals, restructuring, governance, growth, succession or major investment decisions.
- Consultancies and agencies that need independent specialist capability for selected client projects without expanding permanent headcount.

What this is not

- A software-reselling proposition.
- Generic IT support or managed services.
- A replacement for legal advice, statutory audit, reserved legal activity or other regulated professional work.
- A requirement for the professional firm to hand over the client relationship.

2. How the partnership can work

The delivery model can be adapted to the firm, the client and the engagement. Typical structures are:

Specialist subcontract. The professional firm contracts with the client and instructs Sienda for a defined workstream.

Joint delivery. The professional firm and Sienda work visibly alongside one another, each within a defined remit.

White-label / behind-the-scenes support. Where appropriate, Sienda performs specialist analysis and produces working papers or deliverables for the professional firm to incorporate into its own engagement.

Direct specialist engagement by referral. Where commercially and professionally appropriate, the client engages Sienda directly while the referring firm retains its own advisory role.

PROFESSIONAL BOUNDARY

Where an engagement raises questions requiring legal interpretation or reserved legal work, those questions remain with the instructing law firm or appropriately qualified adviser. Sienda's remit is the operational, organisational, governance, technology and risk analysis that supports the professional advice.

3. Services at a glance

	SERVICE	WHAT IT SOLVES
1	AI Governance & Regulatory Readiness	Controls how AI is selected, used, governed and evidenced.
2	Digital & AI Due Diligence	Finds digital red flags before an acquisition, disposal or investment.
3	Organisational Architecture & AI Readiness	Tests the organisation before automating it.
4	Group Digital Governance	Creates common rules for data, AI, systems and suppliers across a group.
5	Digital Continuity & Key-Person Risk	Reduces dependency on founders, individuals and undocumented digital knowledge.
6	Cyber & Operational Resilience	Strengthens governance, continuity, incident response and supplier resilience.
7	Data Governance & Digital Compliance	Brings legacy privacy/data governance into line with today's cloud and AI environment.
8	Technology Investment & Vendor Due Diligence	Independent review before a major technology commitment is signed.
9	AI Transformation Programme	Takes AI from business diagnosis to governed implementation and measurable outcomes.
10	Post-Merger Digital Integration	Day 1 / Day 100 integration of systems, data, access and suppliers after a deal.
11	Data Asset & Data Access Governance	Identifies who controls business data and how it can be used, shared and protected.
12	ICT Third-Party Risk & Financial Operational Resilience	Structured third-party and operational-resilience governance for regulated financial firms.

SERVICE 1 | AI / GOVERNANCE / RISK

AI Governance & Regulatory Readiness

Establishes how an organisation selects, uses, controls and evidences artificial intelligence across the business.

Best suited to

Businesses already using generative AI or embedded AI, organisations introducing AI into operational processes, employers using AI in recruitment or workforce management, and regulated organisations where AI use creates material compliance or reputational risk.

Typical scope

- AI inventory and use-case mapping
- approved and unapproved AI tools, including shadow AI
- ownership, accountability and escalation
- risk classification and human oversight
- AI policies and acceptable-use rules
- data protection and automated decision-making
- supplier and AI-vendor governance
- staff guidance, training and AI literacy
- documentation, evidence and periodic review

Typical deliverables

AI inventory; governance map; AI policy suite; risk and control register; supplier review framework; training brief; remediation roadmap.

UK regulatory context

- The UK does not currently have a single general AI Act. The relevant framework may draw on the [UK Government's pro-innovation AI regulatory approach](#).
- Where personal data is involved: [UK GDPR](#), [Data Protection Act 2018](#) and [Data \(Use and Access\) Act 2025](#).
- Depending on use: [Equality Act 2010](#) and sector-specific regulation may also be relevant.
- For UK organisations with relevant EU activities: the [EU Artificial Intelligence Act](#) may require separate assessment.

SERVICE 2 | M&A / DEALS / RED FLAGS

Digital & AI Due Diligence

Provides an independent assessment of technology, data and AI risk before an acquisition, disposal, investment or other corporate transaction.

Best suited to

Corporate transactions, private investments, management buy-outs, business sales and situations where systems, data, software or digital operations are material to the value of the target.

Typical scope

- critical systems and infrastructure
- software licences and technology ownership
- cloud dependencies and key suppliers
- cybersecurity and data-protection exposure
- AI systems and automated processes
- intellectual property and digital assets
- legacy systems and technical debt
- vendor lock-in and continuity risk
- likely post-completion remediation and investment

Typical deliverables

Red-flag report; risk register; priority remediation actions; estimated investment areas; Day 1 / Day 100 issues list.

UK regulatory context

- There is no statutory service called “Digital & AI Due Diligence”. The review tests potential exposure under relevant regimes, which may include [UK GDPR](#), [Data Protection Act 2018](#), [Data \(Use and Access\) Act 2025](#) and [Network and Information Systems Regulations 2018](#).
- For regulated financial targets, [FCA operational resilience requirements](#) and [PRA outsourcing and third-party risk expectations](#) may also be material.

SERVICE 3 | ORGANISATION / AI / OPERATING MODEL

Organisational Architecture & AI Readiness

Determines whether the organisation itself is ready for AI before technology is introduced, so that weak structures and inefficient processes are not simply automated.

Best suited to

Established SMEs, professional firms, groups, growing businesses and management teams considering substantial AI or automation investment.

Typical scope

- organisational structure and decision rights
- roles, responsibilities and accountability
- process and information-flow mapping
- duplication, bottlenecks and manual controls
- data availability and quality
- dependencies on individuals
- current systems and integration constraints
- automation and AI opportunity identification

Typical deliverables

Organisational diagnostic; responsibility map; process issues register; AI-readiness assessment; prioritised opportunity portfolio; recommended operating-model changes.

UK regulatory context

- This is primarily an organisational advisory service. Relevant governance considerations can include directors' duties under the [Companies Act 2006](#).
- Where AI processes personal data or affects individuals: [UK GDPR](#), [Data Protection Act 2018](#), [Data \(Use and Access\) Act 2025](#) and, depending on the use case, [Equality Act 2010](#).

SERVICE 4 | GROUPS / HOLDINGS / CONTROL

Group Digital Governance

Creates a common governance model for data, AI, systems, suppliers and technology risk across multiple group entities.

Best suited to

Holding companies, corporate groups, businesses operating through several legal entities and organisations that have grown through acquisition.

Typical scope

- group versus subsidiary responsibilities
- data ownership and information flows
- AI governance and technology standards
- identity and access-management principles
- supplier and cloud governance
- cybersecurity responsibilities
- shared services and minimum controls
- escalation and management reporting

Typical deliverables

Group digital-governance framework; RACI/responsibility matrix; minimum-control standard; data/AI governance principles; reporting and escalation model.

UK regulatory context

- No single UK statute governs “Group Digital Governance”. Depending on the group, relevant requirements can arise under the [Companies Act 2006](#), [UK GDPR](#), [Data Protection Act 2018](#), [Data \(Use and Access\) Act 2025](#) and [Network and Information Systems Regulations 2018](#).

SERVICE 5 | SUCCESSION / CONTINUITY / KEY PEOPLE

Digital Continuity & Key-Person Risk

Identifies and reduces operational dependence on founders, directors, employees or suppliers who hold critical digital access, knowledge or control.

Best suited to

Owner-managed businesses, family businesses, partnerships, succession situations, rapidly growing SMEs and businesses with concentrated operational knowledge.

Typical scope

- administrator accounts and privileged access
- domains, cloud environments and digital assets
- critical software and supplier relationships
- undocumented procedures and business knowledge
- data locations and recovery arrangements
- licences, delegated authorities and approval dependencies
- handover, backup responsibility and recovery procedures

Typical deliverables

Key-person dependency map; critical-access register; continuity gaps; handover requirements; remediation plan; governance recommendations.

UK regulatory context

- For most businesses this is a governance and continuity engagement, not a standalone statutory requirement. Additional obligations may arise under the [Network and Information Systems Regulations 2018](#) or, for financial firms, [FCA operational resilience requirements](#).

SERVICE 6 | CYBER / CONTINUITY / INCIDENTS

Cyber & Operational Resilience

Assesses whether an organisation can prevent, withstand, respond to and recover from serious digital or operational disruption.

Best suited to

Essential and digital service providers, regulated organisations, critical suppliers, managed-service providers and businesses where technology disruption could materially affect operations or customers.

Typical scope

- governance and management accountability
- risk-management structure
- incident management and escalation
- business continuity and recovery
- critical suppliers and dependencies
- backup and restoration governance
- reporting and evidence
- remediation programme and management oversight

Typical deliverables

Resilience assessment; incident and escalation framework; continuity-control map; supplier-risk actions; remediation plan; management reporting structure.

UK regulatory context

- The current UK cyber-resilience framework for organisations within scope includes the [Network and Information Systems Regulations 2018](#).
- The proposed [Cyber Security and Resilience \(Network and Information Systems\) Bill](#) is progressing through Parliament and is intended to reform and expand the existing regime. Until enacted, it should be treated as a readiness consideration rather than a current statutory obligation.

SERVICE 7 | DATA / PRIVACY / DIGITAL CHANGE

Data Governance & Digital Compliance

Tests whether historic privacy and data-governance arrangements still reflect the way the organisation actually operates today.

Best suited to

Organisations whose GDPR work was completed several years ago, businesses that have materially increased cloud, SaaS or AI use, groups and rapidly changing businesses.

Typical scope

- data-processing reality versus historic documentation
- cloud and SaaS applications
- AI and automated decision-making
- processor and supplier relationships
- international data flows
- retention and access control
- shadow IT and shadow AI
- governance ownership and evidence
- priority remediation

Typical deliverables

Current-state data-governance assessment; gap register; processing and supplier issues list; governance updates; remediation roadmap.

UK regulatory context

- Key legislation includes the [UK GDPR](#), [Data Protection Act 2018](#) and [Data \(Use and Access\) Act 2025](#).

SERVICE 8 | INVESTMENT / VENDORS / PROCUREMENT

Technology Investment & Vendor Due Diligence

Provides independent challenge before a business signs a major technology, cloud, AI, software or outsourcing commitment.

Best suited to

Organisations preparing to commit significant capital, operational dependency or strategic change to an ERP, CRM, AI platform, cloud migration, bespoke software or major outsourcing arrangement.

Typical scope

- business requirements and expected outcomes
- supplier capability and delivery assumptions
- commercial model and recurring costs
- data ownership and control
- integration and implementation risk
- security and privacy implications
- vendor lock-in and concentration risk
- termination, exit and continuity provisions

Typical deliverables

Independent investment review; vendor-risk findings; commercial and operational red flags; decision questions; contract/implementation issues list for the professional advisers; recommended controls.

UK regulatory context

- There is no general statutory requirement to perform technology-investment due diligence. Specific obligations can arise under the [UK GDPR](#) for processor relationships and under the [Network and Information Systems Regulations 2018](#) for organisations within scope.
- For financial firms, relevant expectations include [FCA outsourcing and operational resilience requirements](#) and [PRA Supervisory Statement SS2/21 on outsourcing and third-party risk management](#).

SERVICE 9 | STRATEGY / AI / IMPLEMENTATION

AI Transformation Programme

Takes AI from business diagnosis through use-case selection, business case, governance, vendor choice, implementation oversight and measurement.

Best suited to

Boards and management teams considering substantial AI adoption and organisations that want measurable business outcomes rather than disconnected AI experiments.

Typical scope

- business and operating-model diagnostic
- AI opportunity portfolio
- business case and prioritisation
- governance and control design
- vendor/solution assessment
- implementation oversight
- benefit realisation and outcome measurement

Typical deliverables

AI transformation roadmap; prioritised business cases; governance model; vendor/solution assessment; implementation-control plan; outcome measures.

UK regulatory context

- There is no statutory requirement to undertake an “AI Transformation Programme”. The applicable legal context depends on the use case and may include the [UK GDPR](#), [Data Protection Act 2018](#), [Data \(Use and Access\) Act 2025](#) and [Equality Act 2010](#).
- For relevant EU-facing activity, the [EU Artificial Intelligence Act](#) may also need to be assessed.

SERVICE 10 | M&A / INTEGRATION / DAY 100

Post-Merger Digital Integration

Provides a structured Day 1 / Day 100 programme for integrating the digital and operational environments of businesses following an acquisition or merger.

Best suited to

Acquirers, corporate groups, private-equity portfolio companies and professional advisers supporting post-transaction integration.

Typical scope

- systems and user accounts
- identity and access
- data and cloud services
- software licences and suppliers
- cyber and privacy governance
- AI systems and digital assets
- business continuity
- duplicate technology and migration priorities

Typical deliverables

Day 1 readiness plan; Day 100 integration roadmap; systems/data dependency map; access and supplier actions; risk register; governance and migration priorities.

UK regulatory context

- There is no specific statutory requirement for “Post-Merger Digital Integration”. Relevant legal and regulatory considerations may arise under the [Companies Act 2006](#), [UK GDPR](#), [Data Protection Act 2018](#) and, for organisations within scope, the [Network and Information Systems Regulations 2018](#).

SERVICE 11 | DATA ASSETS / ACCESS / VALUE

Data Asset & Data Access Governance

Helps an organisation understand what data it possesses, where it originates, who controls it, who may use it and where commercial or governance value is being lost.

Best suited to

Technology businesses, manufacturers, platforms, connected-product businesses, data-intensive companies and organisations exploring data-sharing or monetisation opportunities.

Typical scope

- data-asset inventory
- ownership and control
- connected-product and IoT data
- third-party access and data-sharing arrangements
- APIs and portability
- contractual rights and restrictions
- commercial use opportunities
- governance and accountability

Typical deliverables

Data-asset map; access/control matrix; contractual issue list for professional advisers; governance model; opportunity and risk register.

UK regulatory context

- The UK framework may include the [Data \(Use and Access\) Act 2025](#), [UK GDPR](#) and [Data Protection Act 2018](#) alongside contractual and intellectual-property considerations.
- Where a UK organisation supplies connected products or related services into the EU, separate assessment of the EU Data Act may also be required.

SERVICE 12 | FINANCIAL SERVICES / THIRD PARTIES / RESILIENCE

ICT Third-Party Risk & Financial Operational Resilience

Provides structured governance of technology suppliers, cloud providers, outsourcing and material third-party dependencies within regulated financial-services organisations.

Best suited to

Banks, insurers, payment firms, investment firms and other organisations within relevant FCA/PRA operational-resilience or outsourcing regimes.

Typical scope

- third-party inventory and criticality
- supplier due diligence
- concentration risk
- cloud and outsourcing dependencies
- contractual controls and exit planning
- ongoing monitoring
- incident and continuity arrangements
- board and management reporting

Typical deliverables

Third-party risk framework; materiality/criticality methodology; supplier register; risk and control assessment; exit/continuity requirements; governance and reporting pack.

UK regulatory context

- Relevant UK requirements include [FCA operational resilience requirements](#), [FCA outsourcing and third-party expectations](#) and [PRA Supervisory Statement SS2/21](#).
- Final FCA/PRA rules for operational-incident and material third-party reporting were published in March 2026 and take effect on 18 March 2027. See [FCA Policy Statement PS26/2](#).

4. When to bring Sienda into a client matter

The professional adviser does not need to diagnose the whole problem. A trigger is enough to start a scoped specialist conversation.

CLIENT TRIGGER	SPECIALIST RESPONSE
<i>"Our client is buying or selling a business."</i>	Digital & AI Due Diligence
<i>"The board wants an AI strategy."</i>	AI Governance & Regulatory Readiness / AI Transformation Programme
<i>"They are using AI everywhere, but nobody owns it."</i>	AI Governance & Regulatory Readiness
<i>"Their GDPR documentation is several years old."</i>	Data Governance & Digital Compliance
<i>"They are about to sign a major ERP, CRM, cloud or AI contract."</i>	Technology Investment & Vendor Due Diligence
<i>"The whole business depends on the founder or one technical person."</i>	Digital Continuity & Key-Person Risk
<i>"The group has multiple companies, systems and inconsistent controls."</i>	Group Digital Governance
<i>"The acquisition has completed; now the systems need to be integrated."</i>	Post-Merger Digital Integration
<i>"A disruption or supplier failure could stop the business."</i>	Cyber & Operational Resilience
<i>"The client is FCA/PRA regulated and heavily dependent on third parties."</i>	ICT Third-Party Risk & Financial Operational Resilience
<i>"They want to automate, but the operating model is unclear."</i>	Organisational Architecture & AI Readiness
<i>"They have valuable data but no clear view of ownership, access or value."</i>	Data Asset & Data Access Governance

5. Engagement process

- 01 Trigger** — Your firm identifies a client matter with a material AI, data, technology, digital-risk or transformation component.
- 02 Scoping** — We hold a short scoping discussion with the professional firm, and with the client if appropriate, to define the question and boundaries.
- 03 Proposal** — Sienda provides a defined scope, deliverables, assumptions, timing basis and commercial terms.
- 04 Delivery** — We perform the analysis, interviews, evidence review, workshops and documentation required by the agreed scope.
- 05 Professional integration** — Findings are delivered to the client directly, jointly, or through the instructing firm, depending on the agreed model.
- 06 Remediation / next phase** — Where needed, a separate implementation, remediation or monitoring workstream can be agreed.

Commercial arrangements

Commercial terms are agreed with the partner firm for each relationship or engagement. They can be structured as subcontracted delivery, project fees, retained specialist support or another agreed commercial model. The intent is to create a commercially useful capability for the professional firm, not merely a referral channel.

Confidentiality and conflicts

Confidentiality, conflicts, information handling, client contact and use of the professional firm's name are agreed before work begins. Where the instructing firm requires a particular engagement protocol, Sienda works within that protocol.

6. Why Sienda

- Business-first approach: technology is assessed in the context of organisation, governance, risk and commercial outcomes.
- Independent of software vendors: recommendations are not driven by licence sales or implementation commissions.
- Cross-functional perspective: AI, data, process, governance, digital risk and commercial decision-making are considered together rather than in isolation.
- Professional-firm friendly: scope, boundaries, client contact and deliverable ownership can be adapted to the instructing firm's engagement model.
- Deliverable-led: engagements conclude with clear findings, evidence, risks, decisions and remediation actions rather than open-ended advisory hours.

OUR ROLE

We help professional firms answer the operational question behind the legal, financial or corporate question: what is actually happening inside the client's organisation, systems, data, AI use and supplier landscape — and what should management do about it?

7. Selected official UK regulatory references

These links are provided as a concise reference point. The applicability of any legislation or regulatory requirement depends on the client, activity, sector and facts of the engagement.

- [UK GDPR — legislation.gov.uk](https://legislation.gov.uk)
- [Data Protection Act 2018 — legislation.gov.uk](https://legislation.gov.uk)
- [Data \(Use and Access\) Act 2025 — legislation.gov.uk](https://legislation.gov.uk)
- [Network and Information Systems Regulations 2018 — legislation.gov.uk](https://legislation.gov.uk)
- [Companies Act 2006 — legislation.gov.uk](https://legislation.gov.uk)
- [Equality Act 2010 — legislation.gov.uk](https://legislation.gov.uk)
- [UK Government: AI regulation — a pro-innovation approach](#)
- [Cyber Security and Resilience \(Network and Information Systems\) Bill — UK Parliament](#)
- [FCA: Operational resilience](#)
- [FCA: Outsourcing and operational resilience](#)
- [FCA PS26/2: Operational incident and third-party reporting](#)
- [PRA SS2/21: Outsourcing and third-party risk management](#)
- [EU Artificial Intelligence Act — EUR-Lex \(where EU activities are relevant\)](#)

8. Starting a partnership

The simplest starting point is a short partner-level discussion around the types of client matters your firm already sees.

We can then identify two or three services that fit your client base, agree how matters should be introduced and scoped, and establish the preferred delivery and commercial model.

Sienda ltd

Business Engineering & Independent Advisory

www.sienda.co.uk

Professional firms interested in discussing potential collaboration, subcontracted delivery or white-label support are welcome to contact Sienda Ltd's Director, Dr. Bob Mazzei, directly at bob@siendaweblines.com

Important: This document is a service proposal, not legal advice. Regulatory references are indicative and must be assessed against the facts and sector of each client engagement.