we complement

Why We Complement Pursued ISO 27001

Information security in practice: why people matter more than policies

Information security is often discussed as if it lives somewhere separate from day-to-day work. In IT teams, in systems, or in policies most people never read.
In practice, information security lives with people.
It lives in how emails are sent, how documents are stored, how access is granted and removed, how questions are raised, and how mistakes are handled when they inevitably occur.
As an outsourced consultancy working closely with financial planning firms, this human reality is impossible to ignore. Our work involves people handling sensitive client information, drafting advice, and supporting decisions that materially affect clients' financial lives.

> *"In practice, information security lives with people."*

That is why we chose to pursue ISO 27001. Not as a technical exercise, and not as a marketing badge, but as a way of embedding better habits, clearer ownership, and stronger accountability into how we operate as people, not just as a business.

Outsourcing makes information security more human, not less

Outsourcing is often framed as an operational or commercial decision. In reality, it is a human one.
When advice firms outsource support, information does not simply move between systems. It moves between people.
Each handover involves judgement. Each access permission relies on trust. Each process depends on someone doing the right thing, consistently, often under time pressure.

Security is shaped by everyday decisions, not just formal controls.

The myth of "technical" information security

ISO 27001 is frequently misunderstood as a technology standard. That misunderstanding often leads firms to underestimate both its scope and its value. While systems and controls matter, the standard is fundamentally concerned with behaviour, ownership, and decision-making.

ISO 27001 asks organisations to demonstrate, in practice:

- Who is accountable for information
- How risk is identified and reviewed
- How access decisions are made and revisited
- How people are trained and supported
- How incidents are handled and learned from

These are human questions first, technical questions second.

This focus is well aligned with the Information Commissioner's Office's own findings, which consistently show that the majority of data incidents arise from human error rather than malicious attack.

ICO guidance on data security and human risk.

Why this mattered to us

As an outsourced consultancy supporting financial planning firms, we had to be honest about the role we play in the advice ecosystem.

We handle sensitive information every day. Draft suitability reports, client financial data, internal firm processes, and strategic documentation. That information passes through multiple hands, across different engagements, often at pace.
Pursuing ISO 27001 forced us to look beyond policy statements and ask more searching questions.

Not what we intend to do, but what actually happens.
Not what should happen in theory, but what happens under pressure.
Not who is responsible in name, but who is accountable in reality.

That level of scrutiny is uncomfortable. It is also essential.

What ISO 27001 actually required in practice

ISO 27001 is a formally audited information security management standard. Achieving it requires organisations to evidence how information security operates across the whole business, not just describe it.

This meant demonstrating, with evidence:

- How we identify and assess information security risk
- How ownership and accountability are assigned
- How controls reflect real working practices, not idealised ones
- How all team members are trained, not just senior or technical staff
- How access to information is granted, reviewed, and removed
- How incidents, near-misses, and questions are recorded and reviewed
- How we monitor, test, and improve controls over time

This was supported by independent external audits that tested behaviours as well as documentation. Auditors explored how decisions were made, how exceptions were handled, and how we ensured controls remained effective as the business evolved.

> *"We had to evidence discipline, consistency, and learning, not just good intentions."*

For a people-led service business, this level of scrutiny is demanding. It does not allow information security to sit quietly in policies or systems. It requires it to be lived day to day by real people doing real work.

Why ISO 27001 is rare in outsourced adviser support

Many outsourced support firms are staffed by experienced, conscientious professionals. That alone does not guarantee consistency or resilience, particularly as teams grow and workloads increase.

ISO 27001 requires organisations to demonstrate that good practice does not rely on individual judgement alone, but is supported by structure, training, oversight, and review.

In practice, this means evidencing:

- Consistency across teams and clients
- Clear escalation and accountability
- Ongoing assessment rather than one-off fixes

For service firms built around people, this level of formalisation can feel onerous. It is also why relatively few choose to pursue it.

Practical reflections for advice firms

When reviewing outsourced arrangements, firms may find it useful to reflect on how human risk is managed in practice.

Some questions worth asking:

1. How are people trained to handle sensitive information day to day?
2. How is access reviewed as roles and responsibilities change?
3. How are mistakes encouraged to be reported and learned from?
4. Who is accountable if something goes wrong?
5. How do we know controls still work as the business grows?

These are governance questions, not technical ones.

The FCA's expectations under the Senior Managers and Certification Regime reinforce the importance of clear accountability across all outsourced activity.

FCA guidance on the Senior Managers and Certification Regime

What ISO 27001 changed, and what it confirmed

Pursuing ISO 27001 did not fundamentally change who we are or how we approach our work.

What it did was force us to evidence and formalise practices that already mattered to us, and to test whether they held up consistently under independent scrutiny.

In some areas, it confirmed that our instincts and habits were sound. In others, it highlighted where too much reliance was placed on individual experience rather than shared structure.

The process helped us:

- Make ownership more explicit rather than assumed
- Document decisions that were previously informal
- Reduce dependency on individual knowledge
- Introduce clearer review and escalation points

Most importantly, it ensured that our approach to information security is not reliant on good people doing the right thing, but supported by governance, training, and oversight that stands up as the business grows. For a consultancy built around people, this distinction matters.

"Good practice should not rely on good people doing the right thing."

In summary

Information security is not a technical hurdle to be cleared once. It is a human discipline that must be practiced continuously.

Our decision to pursue ISO 27001 was rooted in a belief that outsourced support firms should hold themselves to the same standards of accountability and care that financial advisers are expected to demonstrate.

Not because regulation demands it.
Because trust demands it.