ISO SECURITY · ISOSECURITY.CO.UK

How to choose an ISO 27001 consultant

How to choose an ISO 27001 consultant in the UK: who does the work, what the fee includes, independence from the certification body and the warning signs.

Source: https://www.isosecurity.co.uk/resources/how-to-choose-an-iso-27001-consultant

IN THIS GUIDE

What matters most when choosing an ISO 27001 consultant? · Who will actually do the work? · Are they qualified, and in what? · What does the fee include, and what does it leave out? · How does the consultant protect independence from the certification body? · Will the documents be written around your organisation? · Is support at the certification audit included? · What happens after you are certified? · What are the warning signs? · How do my answers compare? · Frequently asked questions about choosing an ISO 27001 consultant · Contact

Two ISO 27001 quotes can look similar and describe very different work. These questions show who will do the work, what the fee covers and whether the advice stays independent.

What matters most when choosing an ISO 27001 consultant?

Five things: who does the work, what they have audited as well as built, what the fee includes, how independence from the certification body is protected, and what happens after the certificate. The table shows what to listen for, and the sections below take each in turn.

Question	A good answer	A warning sign
Who will do the work?	A named person who runs your workshops and writes your documents	A senior name in the sale and unnamed juniors in delivery
What is their background?	Lead Implementer and Lead Auditor credentials you can verify	Credentials in implementation only, or none you can check
What does the fee include?	A written scope covering documents, workshops, internal audit and audit support	A single figure quoted before anyone asked about your scope
How is independence kept?	You contract and pay the certification body separately	The certificate bundled into the consultancy price
What happens afterwards?	A clear plan for surveillance audits and for who owns the system	Silence about years two and three
What do they promise?	Honest ranges for time and cost, with the decision left to the certification body	A promised certification result, or a fixed number of days

Who will actually do the work?

Ask who writes your documents, who runs the risk workshops and who sits beside you at the audit. A senior name in the sales conversation does not tell you who delivers.

Senior-led and delegated models can both work, provided you know which one you are buying. Insist on a named person, and ask how much of the project that person does personally.

Are they qualified, and in what?

Look for implementation and audit credentials together. A consultant who has also been an auditor knows what will be tested and builds that in from the start.

Ask for the credential names and certificate details so that you can verify them with the issuing body, and ask about experience in organisations of your size and sector. Published case studies show the scope and approach behind a claim.

What does the fee include, and what does it leave out?

Ask for the scope in writing: the gap analysis, risk assessment, Statement of Applicability, policies, internal audit and support at the certification audit. Then ask what happens if the audit raises findings.

A fixed fee is easier to compare than a day rate, as long as the scope is clear. My fees are published on the pricing page, and my cost guide lists what other UK providers publish.

How does the consultant protect independence from the certification body?

The certification body audits you and issues the certificate, and it must stay independent of whoever built your system. For that reason you contract and pay the certification body yourself.

Treat any quote that bundles the certificate into consultancy with caution. A consultant can prepare you, but nobody who helped build the system can audit and certify it.

Will the documents be written around your organisation?

Auditors test whether what is written matches what people actually do. A generic pack of documents will not survive that test.

Ask who sets the risk scores. Registers that arrive pre-scored carry somebody else's risks, and your managers will be asked to explain them. My consultant versus toolkit guide covers this in detail.

Is support at the certification audit included?

Ask whether support at the audit itself is part of the fee, and what happens if the auditor raises findings. A major nonconformity must be closed before certification, so the help you receive around the audit matters.

My guides to Stage 1 and Stage 2 and to how findings are graded explain what to expect.

What happens after you are certified?

Certification runs in a three-year cycle with surveillance audits in between. Ask who will keep the system running, and what that costs.

Some organisations assign an internal owner and buy help for internal audit and audit preparation, while others bring in a virtual CISO. Either way, decide before you start: my guide to who should own your ISMS explains why most post-certification failures trace back to an ownership vacuum.

What are the warning signs?

- **A guaranteed result.** Certification bodies typically look for around three months of operating records before Stage 2, and the certification decision is theirs.
- **A price without questions.** Anyone quoting you a single figure without asking about your scope is guessing.
- **Pre-filled documents.** Risk registers and policies that nobody adapted to how you work will not hold up at audit.
- **No named person.** If nobody can tell you who will do the work, you cannot judge their experience.
- **A bundled certificate.** The certification body must be contracted and paid separately.
- **Nothing about year two.** A consultant who says nothing about surveillance audits or ownership has not planned beyond the first certificate.

How do my answers compare?

These are my answers to the same questions, so that you can set them beside any other quote.

- **Who does the work.** I lead every engagement personally, from the first conversation through to certification and ongoing support.
- **Background.** I am a certified ISO 27001 Lead Implementer, a certified Lead Auditor and a CISSP, and ISO Security has been established since 1995.
- **The fee.** Implementation is a fixed fee once scope is established, and the bands are on my pricing page.
- **Independence.** ISO Security is a consultancy, and I cannot audit and certify a system I helped build. You contract the certification body directly, and I help you select and engage an accredited one.
- **Evidence.** My case studies cover Inmarsat, Chaucer, Lean Tree and a UK charity.
- **After certification.** Ongoing support starts from £850 a month, and if the honest answer is that your own team can run it, I will tell you so.

Frequently asked questions about choosing an ISO 27001 consultant

How much should an ISO 27001 consultant cost?

Published UK implementation fees range from about £7,500 for a fully assisted fixed-fee offer to £25,000 or more for senior-led programmes, and my own fees run from £10,000 to £38,000 by organisation size. Compare who does what on each quote, because price-only comparisons are how organisations end up paying twice.

Do we need an ISO 27001 consultant at all?

Not always. A capable internal owner with protected time can succeed on a simple scope, and my consultant versus toolkit guide costs each route in money and internal hours.

Can the same company implement and certify ISO 27001?

No. The certification body must stay independent of whoever built the system, so a consultancy cannot certify a system it helped create.

Should an ISO 27001 consultant be local to us?

Not necessarily. Most of the work can be delivered through remote workshops and reviews, with on-site time where it adds value, and I work with organisations across the UK.

What if we already have an ISMS and want a different consultant?

That is one of the most common reasons organisations contact me. I start with a mobilisation review of the existing system and, where possible, a handover with your previous consultant. See taking over an existing ISMS.

What should I ask a consultant on the first call?

Ask who will do the work, what the fee includes and leaves out, how independence from the certification body is protected, whether support at the audit itself is included, and who will own the system afterwards.

Contact

Want to put these questions to me? Arrange a readiness discussion: contact ISO Security or email info@isosecurity.co.uk.

> **Arrange a readiness discussion** — tell ISO Security where you are today and get a clear view of the work and investment required.
> Contact: info@isosecurity.co.uk · https://www.isosecurity.co.uk/contact