ILLUMEN · A FIELD GUIDE

What to Expect When You're Expecting an ISO 27001 Audit

A calm, phase-by-phase guide to certification,
for the person who has to run it

How to read this

Somebody has decided your company is getting certified, and somebody has decided that you are the one who will make it happen. You may have volunteered. You may have been in the wrong meeting.

Either way you are now responsible for a process that runs about a year, involves strangers reading your documents, and ends with a certificate your sales team has already started promising to customers. Nobody has explained the sequence to you. The standard itself is nineteen pages of careful, joyless prose that describes what must be true without ever describing what will happen to you.

This book describes what will happen to you.

It is organised the way the process actually unfolds, in five phases, and each phase follows the same shape: what is happening, what you may be feeling, what your auditor is actually doing, the questions you are too embarrassed to ask, and the one thing per phase serious enough to stop and deal with.

You do not have to read it in order. Find the phase you are in and start there.

> **A NOTE ON THE GENRE**
>
> Yes, this is shaped like a pregnancy guide. The joke is load-bearing. Both processes are long, unfamiliar, full of appointments with professionals who use vocabulary nobody explained, and enormously improved by someone telling you which of the alarming things are normal.

The one idea

If you take nothing else from this book, take the following.

A major nonconformity is expected at Stage 1 and fatal at Stage 2.

That sentence is the whole standard's temperament in miniature. The same finding, the same words in the same report, is either a completely routine part of the process or the thing that stops your certification, depending only on when it turns up.

Almost every painful ISO 27001 outcome is a right thing happening at the wrong moment. Excellent security controls introduced three weeks before the auditor samples them. A perfectly good internal audit that nobody put in front of the person who needed to see it. A policy set that was approved on time, by the right person, in a system whose PDF export still says DRAFT.

None of those are security failures. All of them cost real money and real weeks.

The rest of this book is that sentence, elaborated.

ACT ONE

Conception

You decide to do this. Nobody is watching yet.

Act One: Conception

What is happening this phase

You are not building security. You are building a management system that can prove security happens on purpose.

This distinction sounds like pedantry and is in fact the entire reason first-time programs fail. Plenty of companies with genuinely good security fail their first audit, because what gets assessed is not whether your engineers are careful. It is whether there is a system that would notice if they stopped being careful.

ISMS · Information Security Management System

The machine that runs your security, as opposed to the security itself. It is a set of decisions about scope, risk, ownership and review, written down and actually operated.

The certificate is awarded to the ISMS. Not to your firewall, which nobody will ever ask to see.

Four artefacts do most of the work in this phase. A scope statement that says what is in and what is out. An information security policy signed by someone senior enough to matter. A risk methodology with a completed risk assessment sitting behind it, not just the methodology on its own. And the Statement of Applicability.

SoA · Statement of Applicability

A document listing all 93 Annex A controls, marking each one applicable or not, and justifying the answer. All 93. Not the ones you liked.

The only document in the standard graded on whether you were honest about the ones you skipped.

Annex A

The catalogue of 93 controls at the back of the standard, grouped into organisational, people, physical and technological. Distinct from Clauses 4 to 10, which are the management system itself.

Everyone prepares for Annex A. Clauses 4 to 10 are where the certificate is actually won and lost.

What you may be feeling

That this is a documentation exercise wearing a security exercise as a costume. That you already have the controls and what you lack is the paperwork, and that the paperwork is the part being graded.

Both of those feelings are accurate. Neither is a problem yet. The paperwork is being graded because paperwork is the only durable evidence that a decision was made deliberately rather than by accident, and an auditor who has been in the building for six hours has no other way to tell the difference.

The instructions were in the box the whole time.

What your auditor is actually doing

Nothing. Nobody is watching this phase.

That is precisely why it is the phase most often done badly. Every other phase in this book has an external deadline attached to a person who will show up and ask questions. This one has none, which means it expands to fill the time available and then gets compressed into the fortnight before Stage 1.

What you may be wondering

Do I have to scope in the whole company?

No. But every exclusion has to be defensible and written down, and the defence has to survive a stranger reading it. "That department does not touch customer data" is a defence. "That department was difficult to work with" is not, however true.

Can I just buy the policies?

You can, and an experienced auditor will identify a purchased policy set inside ten minutes. Not because template policies are forbidden, but because the template describes a company you are not.

The specific danger is a policy that claims a control you do not operate. That is not a gap. A gap is honest and gets you a finding. A policy asserting a regime that does not exist is a misrepresentation, and a certification auditor who finds one will stop and start wondering what else is decorative.

How do I know when this phase is finished?

When someone who did not write the documents can read them and correctly describe how your company manages security. If the documents only make sense to their author, you have written notes, not a management system.

> **WHEN TO CALL YOUR PRACTITIONER**
>
> Your policy set claims a control you do not operate. Fix it before anyone external reads it. This is the one Act One mistake that compounds through every phase that follows, because it damages the auditor's trust in every other document you hand them.

ACT TWO

The First Scan

Someone looks properly for the first time.

Act Two: The First Scan

What is happening this phase

The standard requires you to audit yourself before anyone else does. This is not a courtesy or a best practice. It is Clause 9.2, it is mandatory, and arriving at certification without one is a finding before the auditor has asked a single question.

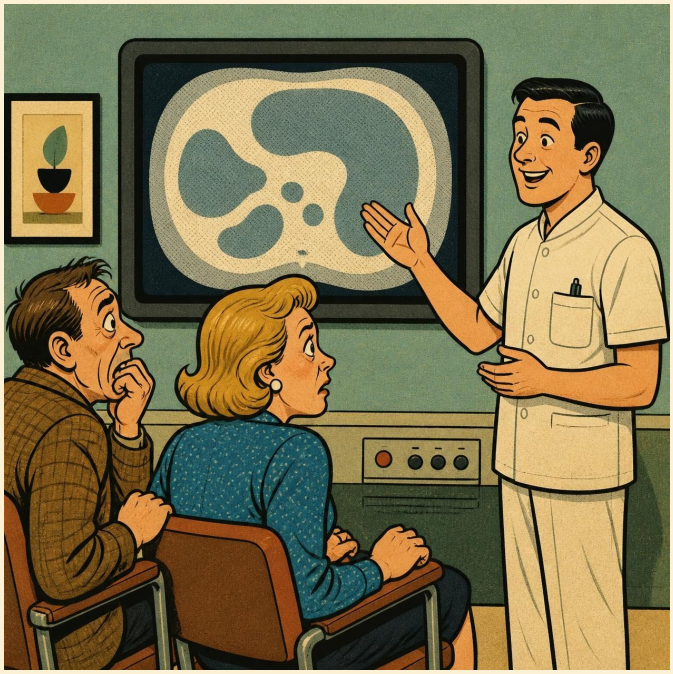
> **Clause 9.2** · Internal audit
>
> The requirement to run your own audit programme against the standard, at planned intervals, using auditors who are objective about what they are auditing.

This is the one phase where finding things is unambiguously good. Every finding you surface here is one the certification body does not get to write down. You are, in a real sense, buying findings at a discount.

What you may be feeling

Defensive. Someone is producing a list of things wrong with work you did, and the instinct is to negotiate the list shorter.

That instinct is exactly backwards, and this is the moment to say so plainly. A short internal audit report is not a good result. It is either a well-run program or a badly run audit, and at this stage you cannot tell which, so the finding you argue away is the finding you meet again in six months with a stranger's name on it.



Most of what shows up on the scan is supposed to be there.

What your auditor is actually doing

Testing your evidence rather than re-auditing your build. Two habits give this away, and recognising them will change how you prepare.

The first is that a good auditor asks to be shown things rather than told things. The request to share your screen is not suspicion. It is the difference between evidence and assertion, and it is faster for everyone.

The second is that a good auditor gives credit before probing. When they open by saying that one part of your programme is genuinely strong, they are not softening you up. They are establishing what already works so the conversation can be about the remainder.

A short internal audit report is not a good result.

What you may be wondering

Can our own team run it?

Only if they can audit work they did not do. Independence under Clause 9.2.2 is about who audits what, not about whether you hire someone.

The same rule binds your consultant, and this is worth knowing before you need it. Whoever designed your ISMS cannot then audit it. If a firm offers to build your program and audit it, they are offering you a finding.

> **Independence**
>
> The requirement that an auditor be objective about the thing they are auditing, which in practice means they did not build it, own it, or get measured on it.

We fixed it during the audit. Does the finding go away?

No, and this is the most misunderstood mechanic in the entire process.

A corrective action taken after the audit closes does not alter a finding that was substantiated by evidence during it. The fix gets recorded, and the record shows a system that identifies and resolves problems, which is exactly what the standard wants. But the finding stands, because the finding is a statement about what was true when it was observed.

Teams find this genuinely unfair the first time. It stops feeling unfair the moment you consider the alternative, which is an audit that can be edited by whoever fixes things fastest during the closing meeting.

How many findings is too many?

Wrong question, and asking it will make your program worse.

Findings are not independent events; they cluster into root causes, and first-time management systems collapse into remarkably similar clusters: approve the document set, run a real risk assessment, correct the Statement of Applicability, hold a management review. Twenty-five findings across four root causes is four weeks of work. Six findings across six root causes may be worse.

> **Nonconformity, major and minor**
>
> Major: the requirement is absent, or the breakdown is systemic. Minor: the requirement is partially met, or the lapse is isolated.
>
> *Absence versus partial. That is the whole test, and where it lands changes what the finding costs you.*

OFI · Opportunity for Improvement

The requirement is met and could be met better. No mandatory timeline, no obligation to act.

Free advice from someone who has seen a hundred of these. Read them.

WHEN TO CALL YOUR PRACTITIONER

You are about to book Stage 1 because the documents are approved, without having completed the internal audit. Do not. Document approval is roughly a third of what Stage 1 examines, and booking on it alone is the most reliable way to convert your own manageable findings into someone else's permanent record.

ACT THREE

The Twelve-Week Appointment

Stage 1. The one everyone misunderstands.

Act Three: The Twelve-Week Appointment

What is happening this phase

An external certification body reads your management system and forms a view on whether it exists, hangs together, and is ready to be tested properly.

Certification body

The accredited organisation that audits you and issues the certificate. Distinct from your consultant, who cannot do this, and from your customer, who will ask for it.

Stage 1

A documentation and readiness review. The auditor walks your scope, policy, risk methodology, completed risk assessment, Statement of Applicability, internal audit results and management review evidence, then Clauses 4 to 10.

What you may be feeling

Convinced this is the real exam.

It is not, and the misapprehension does measurable damage. Teams over-prepare for Stage 1, spend themselves completely, take the win, rest for a month, and then arrive at Stage 2 with three weeks of operating records and nothing to sample.

Read this next sentence twice, because it is the most reassuring true thing in the book.

> **Nobody fails Stage 1 for having gaps. Finding them is what Stage 1 is for.**

Major nonconformities at Stage 1 are expected. The room is not adversarial. The auditor is not deciding whether you deserve a certificate, they are deciding whether it is worth anyone's time to run Stage 2 yet.

Everyone else in the waiting room seems fine about this.

What your auditor is actually doing

Reading. Then asking you to explain the parts that do not reconcile.

Most of Stage 1 is spent on the management system rather than the 93 controls, which surprises teams who spent their preparation on the controls. Expect an opening meeting, a walk through the mandatory documents, a conversation about Clauses 4 to 10, a list of findings, and a Stage 2 date.

What you may be wondering

What does a real Stage 1 outcome actually look like?

Here is the shape it usually takes, drawn across a number of first certifications rather than any one of them.

Somewhere between half a dozen and a dozen areas of concern, and often no formal nonconformities at all. Every item written as something to resolve before Stage 2 rather than something blocking.

They tend to fall into three groups. Some are document-state problems, where the content is finished and the revision history table still reads DRAFT. Some are legacy governance documents nobody has opened in over a year. The rest are missing operating records: no management review held yet, no corrective action tracking, no continuity test, an internal audit that cannot be produced on the day.

The first two groups are noise and close in a week. The third group is the real work, and it is reliably the one that decides your gap to Stage 2. Knowing that in advance tells you where to spend it.

Area of concern

Softer than a nonconformity. Something to resolve before the next audit, raised without being formally recorded against you. Not every certification body uses the term.

Vocabulary varies between bodies more than anyone admits. Ask yours what they call things.

Our documents are approved but the revision table is blank. Problem?

Yes, and this one is worth more to you than anything else in this act.

The first group above is exactly this, and it is common enough to expect. Policies genuinely approved, by the right person, at the right time, in the compliance platform. The platform recorded it. The exported PDF did not, so its revision history still said DRAFT.

The work was done. The artefact did not say so. An auditor reads the artefact.

Controlled document

A document whose version, approver and approval date are recorded and current. The control is the record, not the content.

How long should the gap to Stage 2 be?

Long enough to have generated evidence. A useful rule of thumb from real scheduling decisions is around two months of the management system actually running, so there is something to sample.

Too soon and you are thin on records. Too late and you risk losing the auditor who already knows your business to their own calendar, and pushing certification past a date your sales team has promised.

WHEN TO CALL YOUR PRACTITIONER

Something you genuinely completed was not in front of the auditor during the review.

An internal audit can be finished, delivered and thorough, and still generate a finding because it was not in the room. That is the cheapest possible finding to avoid and the most irritating one to receive, and it happens constantly.

ACT FOUR

Delivery

Stage 2. The one that decides it.

Act Four: Delivery

What is happening this phase

The auditor stops reading about your management system and starts testing whether it operates. They will pick a period, pull a sample, and trace it. They will talk to people who are not you.

Stage 2

The evidence and effectiveness audit. Stage 1 asked whether the system is designed. Stage 2 asks whether it ran.

What you may be feeling

Tested. Your staff feel it considerably more than you do, and they are the ones sitting in the interviews.

They only look at a few. They choose which few.

What your auditor is actually doing

Sampling, and this is the mechanical fact the whole act turns on.

Sampling

Selecting a subset of records over a period and tracing each one end to end, on the basis that a system either works across the sample or does not.

A control that began operating three weeks ago has three weeks of evidence. There is no document you can write that fixes this, no policy quality that compensates, and no explanation that makes an auditor sample a period that does not exist. This is the entire reason the gap between Stage 1 and Stage 2 matters.

> **Evidence**
>
> A dated artefact showing a control operated. A screenshot with a timestamp, an exported log, an approval record. Not a description of what normally happens.
>
> *"We do that every quarter" is not evidence. It is a claim about evidence that should exist.*

What you may be wondering

What will they ask my engineers?

Open questions, then follow-ups where the answer was thin. A real sequence looks like: walk me through how a change gets from a laptop to production. What runs on that code automatically along the way. Who else can approve it. Show me the last three.

Notice that all four are conversational, and that the best possible answer to the last one is a shared screen. Your engineers should know this in advance, because a team expecting an interrogation performs badly at a conversation.

What do I tell staff who are terrified?

Four rules, and they are the most useful thing you can circulate before the audit week.

Do not guess. Do not overclaim status, because "approved" when the honest answer is "in final review" costs the auditor's trust for the entire audit and they will find out. Do not answer for someone else. And "let me capture that for our lead rather than guess" is a complete and correct answer that nobody is ever criticised for giving.

Then tell them the thing nobody tells them: the auditor is assessing the management system, not the individual.

What if a finding is just wrong?

Say so, once, with the evidence, calmly. Auditors correct findings on evidence routinely and it is not a confrontation.

What does not work is arguing on interpretation without new evidence. If you cannot produce the artefact, you are not disputing the finding, you are disputing whether it needed evidence.

Corrective action

The documented fix for a finding, including the root cause and a check that the fix worked. Closing a finding requires the check, not just the fix.

WHEN TO CALL YOUR PRACTITIONER

A major nonconformity at Stage 2.

This is the one place in this book where the honest answer is serious. A major at Stage 2 stops your certification until it is resolved, and resolution means evidence that the corrective action worked, not a plan to take one. You will be given a window, usually a matter of months rather than weeks, and possibly a follow-up audit. The outer bound is six months from the last day of Stage 2; miss it and the certification body has to run Stage 2 again.

It is recoverable. Companies recover from it regularly. But this is the point at which you stop managing it around your other work, and it is the reason every earlier phase in this book pushed you to find things sooner.

ACT FIVE

The Fourth Trimester

You are certified. Now you have to live in it.

Act Five: The Fourth Trimester

What is happening this phase

You are certified. The certificate runs three years, with a surveillance audit in year one, another in year two, and a full recertification in year three.

> **Surveillance audit**
>
> A shorter annual audit confirming the management system is still running. The first falls within twelve months of your certification decision, the second about twelve months after that.

The change in what is being assessed is subtler than most teams expect, and it is not that surveillance finally tests effectiveness. Stage 2 already did that. The difference is the period. Stage 2 judged you on the months you had, with a deadline in the room making everyone careful. Surveillance judges you on a whole year in which nobody was watching.

What you may be feeling

Relief, and then some months later a quiet suspicion that everyone has stopped doing the thing.

The suspicion is usually correct, and it is not a security problem. It is administrative drift. Nobody got less careful. The system stopped being run, because the deadline that was making it run has gone.

Somebody is still quietly doing the laundry.

What your auditor is actually doing

Sampling a rotating subset of controls, and working through a fixed list that gets covered every time regardless of what they sample: your internal audits and management review, the actions you took on the previous audit's nonconformities, how you handle complaints, whether the system is actually achieving the objectives you set for it, progress on continual improvement, continuing operational control, any change to scope or structure or risk, and correct use of the certification mark.

Look at what dominates that list. Most of it is the management system rather than the individual controls, which is the opposite of where most teams put their preparation. The controls still get sampled and operational control is on the list every time, so this is a reason to prepare for both, not a reason to relax about the technical half.

What you may be wondering

Is it true they only look at half the controls each year?

No. You will read this in a lot of places and it is not a rule.

Sampling is chosen by your auditor on the basis of risk, of what changed since they last visited, and of what they looked at last time, so that coverage builds across the three-year cycle. There is no fixed proportion in the standard governing certification bodies, and planning around "they will only look at half" works right up until the half they choose is the half that changed.

Is a finding at surveillance dangerous?

A minor is not. You submit a corrective action plan with evidence inside an agreed timeframe and the certificate continues uninterrupted. Most teams assume otherwise and brace for something that is not coming.

A major is more serious and has a clear ladder: a resolution window, often around ninety days, sometimes a follow-up audit. Unresolved, it escalates to suspension, and suspension unresolved becomes withdrawal, at which point you start again. Missing a surveillance audit window entirely can trigger the same ladder on its own, with nothing wrong with your management system at all.

We acquired a company. We shipped something new. Do we tell anyone?

Yes, and before the next audit rather than at it.

Most certification agreements carry a contractual duty to notify the body of material change: acquisitions, restructures, new product lines, significant new systems. Two things go wrong when people skip it. Failing to disclose can itself put the certificate at risk. And arriving at a scheduled audit with a scope change nobody knew about means the auditor has not been allocated time to assess it, which converts a routine update into a finding about notification.

What actually lapses first?

The management review, then the corrective action log. Both are calendar items with no external forcing function between audits, which is precisely why they are the most common surveillance findings.

Management review

A recorded meeting where senior leadership reviews how the management system is performing and decides what to change. Required at planned intervals, which in practice means at least annually.

The single most common thing to be missing when the auditor comes back.

WHEN TO CALL YOUR PRACTITIONER

Twelve months have passed and the management review has not been held.

This is the most common surveillance finding there is, and it is entirely a calendar problem. It has no technical cause, no resourcing cause and no complexity. Somebody simply needed to put a recurring meeting in a diary and did not.

A closing thought

The uncomfortable thing about ISO 27001 is that it is not really an assessment of your security. It is an assessment of whether your organisation can hold an intention for longer than a quarter.

That is why the findings in this book cluster where they do. Not around encryption or network architecture, which most engineering teams handle well without being asked, but around the meeting nobody scheduled, the review nobody exported, and the document that was approved in a system whose PDF still said draft.

Which is also, if you have read this far, an oddly reassuring thing to learn. The hard part is not technical. The hard part is calendars, and calendars are a problem you already know how to solve.

When it stops being a calendar problem

Illumen is a boutique GRC firm. We run ISO 27001 internal audits, act as vCISO for companies without a security team of their own, and get organisations through certification with the certification body of their choice.

We are independent auditors, which means we will tell you what we found rather than what is comfortable, and it means we do not audit programs we designed.

If you are somewhere in the five phases in this book and would like a second opinion on where you actually are, we are happy to give you one.

illumen.io · hello@illumen.io

Nobody tells you what an ISO 27001 audit actually feels like from the inside. This is the guide we wish our clients had been handed before their first one: what happens in each phase, what your auditor is really doing, and the one thing per phase that turns a manageable problem into a certification problem.

ILLUMEN · ILLUMEN.IO