TRANCHULAS

PROFESSIONAL TRAINING COURSE

ISO/IEC 27001:2022 ISMS Implementation Masterclass

Design, implement, evidence and sustain a certification-ready ISMS

Build a management system that survives the audit — and the three years after it.

3	13	93	6
FOCUSED DAYS	APPLIED MODULES	ANNEX A CONTROLS	WORKSHOP EXERCISES

For the people who have to build the thing and then defend it — implementers working to a certification date, security managers who own the risk decisions, internal auditors who need to test a system rather than confirm it exists, and the engineers and suppliers actually operating the controls.

Explore dates and enrolment at tranchulas.com

CREST CYBER

ISO 27001:2022 is settling in — the landscape keeps moving

ISO/IEC 27001:2022 is now the only edition in play, it carries an amendment most implementers have never read, the foundation vocabulary beneath it was updated in July 2026, and a growing set of European regulation increasingly leans on the same risk and evidence base. A course written before any of that prepares people for an audit that no longer happens.

31 Oct 2025

CLOSED

The 2013 edition is gone

The transition period closed. Every live certificate is now against ISO/IEC 27001:2022, with 93 Annex A controls across four themes rather than 114 across fourteen. Material still teaching the old control structure is teaching a standard nobody is certified to.

In force

AMENDMENT

Amendment 1:2024 quietly changed Clause 4

Published February 2024, the climate-action amendment requires an organisation to determine whether climate change is a relevant issue in its context, and notes that interested parties can have climate-related requirements. It is short and easy to miss: organisations should be prepared to demonstrate the determination has been made, including where climate change is concluded not to be relevant.

3 Jul 2026

PUBLISHED

The foundation vocabulary was updated

ISO/IEC 27000:2026 updates the overview and vocabulary underpinning the ISO/IEC 27000 family — retitling it “Information security, cybersecurity and privacy protection” and aligning risk language with ISO 31000. It is the overview standard: implementers should understand the revised terminology while continuing to implement against the requirements of ISO/IEC 27001:2022 and Amendment 1:2024.

Sep 2026 →

LIVE

One evidence base, multiple demands

The EU Cyber Resilience Act's reporting duty for actively exploited vulnerabilities starts 11 September 2026, with its main obligations from 11 December 2027. DORA has applied to EU financial entities and their ICT providers since 17 January 2025, and NIS2 transposition continues. A well-designed ISMS produces risk and incident evidence that can support what these regimes ask for — without being equivalent to complying with them.

Alongside

INTEGRATE

AI arrived as a management system, not a control

ISO/IEC 42001 gives AI governance its own certifiable standard on the same Annex L structure as ISO/IEC 27001 — which means it can be integrated with an existing ISMS rather than run as a second, contradictory system. Deciding that early is far cheaper than reconciling two management systems later.

The certificate is not the outcome. The outcome is a management system that keeps producing defensible evidence through surveillance audits, re-certification and a landscape that keeps shifting around it — which is a different thing to build, and a different thing to teach.

The right decisions, in the right order

Many failed implementations are not control failures. They are scope failures and sequence failures — decisions taken in the wrong order, then papered over. The course drills the correct sequence and every workshop is scored on it.

CONTEXT | RISK | **TREATMENT** | EVIDENCE | IMPROVEMENT

Scope decides everything downstream

A boundary drawn loosely to look impressive, or drawn tightly to look easy, sets up every later argument with an auditor. Participants write a scope statement, name its interfaces and dependencies, and then defend it — because Clause 4.3 is where the cheapest mistakes and the most expensive ones both get made.

Risk-led, never control-led

The Statement of Applicability is an output of risk treatment, not a checklist filled in first and justified later. Clause 6.1.3 requires controls to be determined by treatment and then compared against Annex A. Reverse that order and the disconnect becomes readily apparent during audit.

Evidence is the deliverable

Auditors sample records, not intentions. Every module ends in an artefact — a scope statement, a risk register entry, an SoA line with its justification, an audit finding with its root cause — written the way it would be handed over, not summarised on a slide.

Built for year two and year three

The certificate is the easy part. Surveillance audits, corrective action closure, re-certification and a moving standards family are where systems quietly decay. The course treats maintenance as the design problem it actually is.

How every workshop runs

01 Frame the decision and the clause that governs it

02 Surface the facts the room does not yet have

03 Take the decision and record who owns it

04 Produce the artefact an auditor would sample

05 Test it against the question the auditor will ask

What an exercise actually looks like

A specimen decision point from Module 5 — reproduced in full, including the shortcut most implementation teams reach for.

THE SITUATION

A SaaS company wants certification in four months. The security team has worked through the 93 Annex A controls, marked 88 as applicable and implemented, and excluded five — all physical — on the basis that the company is remote-first with no office. The Statement of Applicability is drafted and circulating for sign-off. The risk assessment is scheduled for next month.

THE INSTINCTIVE ANSWER

"We already know our controls. We will back-fill the risk assessment so that it matches the SoA."

WHAT MUST BE ESTABLISHED FIRST

- What the ISMS scope boundary actually is, and which assets, people and suppliers sit inside it
- Which risk criteria and acceptance levels were agreed, and by whom, before anything was scored
- Whether each exclusion is justified by risk, or only by the absence of a building
- What evidence exists that each "implemented" control operates, rather than exists on paper
- Who owns the residual risk that the SoA is implicitly accepting on the organisation's behalf

THE DEFENSIBLE POSITION

The SoA is an output, not an input. Clause 6.1.3 requires necessary controls to be determined through risk treatment and then compared against Annex A to verify nothing has been missed — running it backwards produces an SoA whose rationale becomes difficult to defend under audit. And remote-first does not automatically make physical controls irrelevant: physical risk may instead arise in home-working environments, equipment handling, storage media, data centres and supplier premises. Each control must be considered and its applicability justified through the organisation's risk treatment process.

The same organisation returns on day three as a Stage 1 audit interview, with participants defending the decisions they took on day two.

Thirteen modules across three days

Day one establishes context and risk, day two turns risk into controls and evidence, day three audits the result and takes it to certification.

01

ISO 27001 and the ISMS

The 2022 structure, what a certificate actually asserts, and the shape of a realistic implementation.

ORIENTATION

02

Context of the Organisation

Clauses 4.1 to 4.3, the climate determination added by Amendment 1:2024, and the scope boundary.

SCOPE

03

Policy, Governance and Leadership

Clause 5 in practice: policy that constrains decisions, commitment that appears in records.

GOVERNANCE

04

Risk Assessment Fundamentals

ISO 27005 method, asset and threat analysis, and criteria agreed before anything is scored.

RISK WORKSHOP

05

Risk Treatment and the SoA

Treatment options, control selection, and a Statement of Applicability that is an output.

SoA LAB

06

Annex A: Organisational, People, Physical

Fifty-nine controls across three themes — including physical controls that still require consideration in remote-first environments.

CONTROL MAPPING

07

Annex A: Technological Controls

Thirty-four controls across access, cryptography, network, secure development and cloud.

TECHNICAL

08

Documentation and Records

The documented information Clause 7.5 actually requires, under version control an auditor can follow.

DOC PACKAGE

09

Monitoring and Measurement

Clause 9.1 metrics that mean something, and management review that produces decisions rather than minutes.

METRICS

10

Internal Audit Programme

Clause 9.2 planning, independence, evidence sampling and findings that survive challenge.

MOCK AUDIT

11

Incident Management and Continuity

Response, ICT readiness, and where statutory reporting clocks run separately from the ISMS.

RESPONSE

12

Certification and Improvement

Stage 1 and Stage 2, managing the auditor, corrective action, surveillance and re-certification.

CERT PREP

13

Integration, AI and Supply Chain

Running one management system across ISO/IEC 27001, ISO/IEC 42001 and privacy rather than three that contradict each other; supplier and cloud assurance; and the security culture work that decides whether any of it holds.

ADVANCED

Day 1 ISMS foundations and risk assessment · **Day 2** Risk treatment, controls and documentation · **Day 3** Audit, certification and improvement

Module-by-module detail is in the course outline at tranchulas.com

The evidence, and the control set behind it

Certification turns on records rather than intentions. Participants leave having produced the artefacts on the left, mapped against the control set on the right.

Evidence an auditor may sample

Scope statement Clause 4.3

The boundary, with exclusions justified and every interface and dependency named

Risk assessment and criteria Clause 6.1.2

A repeatable method, criteria agreed in advance, and results someone else could reproduce

Statement of Applicability Clause 6.1.3

Every Annex A control included or excluded, each carrying a stated reason

Risk treatment plan Clause 6.1.3

Owners, dates, and residual risk accepted by someone with the authority to accept it

Competence records Clause 7.2

Evidence that the people operating the controls are able to operate them

Monitoring and measurement Clause 9.1

Results showing whether controls work — not merely that they exist

Internal audit programme Clause 9.2

Plan, auditor independence, findings, and evidence of follow-through

Management review Clause 9.3

Minutes showing the required inputs were considered and decisions were taken

Corrective action records Clause 10.2

Root cause, action taken, and verification that the action was effective

Annex A at a glance — 93 controls

Organisational — 37 controls

Policies, roles, supplier and cloud relationships, threat intelligence, and ICT readiness for business continuity.

People — 8 controls

Screening, terms of employment, awareness, disciplinary process, remote working and the reporting of events.

Physical — 14 controls

Perimeters, entry, equipment, storage media and clear desk — and what each one means when there is no office.

Technological — 34 controls

Access, cryptography, network security, secure development, and the additions made in the 2022 revision.

Eleven controls were new in 2022: threat intelligence; information security for cloud services; ICT readiness for continuity; physical security monitoring; configuration management; information deletion; data masking; data leakage prevention; monitoring activities; web filtering; and secure coding.

What participants can do afterwards

Sixteen capabilities across four areas — each one exercised in a workshop and evidenced in an artefact participants take away.

Set the foundations

- Interpret the 2022 clauses and what each one demands as evidence
- Determine context, including the Amendment 1:2024 climate consideration
- Define an ISMS scope boundary that is defensible under questioning
- Write policy and governance that constrains real decisions

Run the risk process

- Conduct an ISO 27005-aligned assessment from asset to scored risk
- Agree risk criteria and acceptance levels before any treatment decision
- Select controls by risk and justify every inclusion and exclusion
- Produce a Statement of Applicability and treatment plan that hold up

Implement and evidence

- Implement controls across all four Annex A themes
- Build the documented information Clause 7.5 requires, under version control
- Establish monitoring, measurement and management review that decide things
- Assemble the evidence pack an auditor will actually sample from

Certify and sustain

- Plan and run an internal audit programme to Clause 9.2
- Grade nonconformities and drive corrective action to verified closure
- Prepare for and manage Stage 1 and Stage 2 certification audits
- Sustain the system through surveillance, re-certification and standards change

Implementation workbook

Thirteen modules with clause references throughout, written to be used during the implementation rather than read once.

Six workshop exercises

Asset inventory, risk treatment, control mapping, documentation, mock internal audit and certification preparation.

Document and evidence templates

Scope statement, risk register, Statement of Applicability, risk treatment plan, internal audit programme and corrective action record.

A standards-watch register

What is changing across the 27000 family and adjacent regulation, with the clause and the module each change affects.

Four roles, one management system

Designed for individual practitioners, and especially powerful when implementation, security, audit and technology teams train together.

ISMS implementers and project leads

The people who have to get a system built, evidenced and through Stage 2.

Information security managers and CISOs

Owners of the risk process, the treatment decisions and the residual risk.

Internal auditors and compliance

Auditors who need to test a system properly rather than confirm it exists.

IT, engineering and supplier management

The people who operate the controls the certificate is asserting.

Questions we are usually asked

"We are already certified."

Then the questions are whether your Clause 4.1 determination covers climate, whether your SoA can be traced back to risk treatment, and whether your last surveillance audit found anything you have actually closed. Certification is a starting position, and the vocabulary beneath it was updated again in July 2026.

"We are remote-first, so physical controls do not apply."

Remote-first does not automatically make physical controls irrelevant — physical risk shifts to home-working environments, equipment, storage media, data centres and supplier premises. Each control still has to be considered and its applicability justified through risk treatment. Module 6 works through that reasoning.

"We will do the risk assessment after we pick the controls."

That reverses Clause 6.1.3. It is a common implementation failure and creates a weak trace between identified risks, treatment decisions and the SoA. Module 5 runs the correct sequence on a live scenario and shows what the backwards version looks like from the auditor's side of the table.

"Certification is a procurement box to tick."

A well-designed ISMS produces risk records, incident evidence and management accountability that also support what regimes like the CRA, DORA and NIS2 require — though certification is not the same as complying with them. Built only to pass an audit, an ISMS does neither well.

TRANCHULAS

Ready to build an ISMS that holds up?

Explore course dates, discuss private delivery for your implementation team, or request enrolment information for the ISO/IEC 27001:2022 ISMS Implementation Masterclass.

WEB

tranchulas.com

EMAIL

info@tranchulas.com