

GLOBAL SKILL DEVELOPMENT COUNCIL (GSDC)

ISO 27001 Lead Auditor Certification (GSDC) Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

ADVANCED

24 HOURS

3 DAYS

LEAD AUDITOR

At a glance

COURSE	ISO 27001 Lead Auditor Certification (GSDC)
TRACK	Global Skill Development Council (GSDC)
DOMAIN	Cyber Security
LEVEL	Advanced
DURATION	24 hours (about 3 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is a advanced course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Ten modules covering the ISO/IEC 27001:2022 lead-auditor body of knowledge and the audit process defined in ISO 19011, taught in the order an audit actually runs.

The certificate is not awarded by the training provider. A lead auditor credential is issued by a certification body, and this course prepares you for the Certified ISO 27001:2022 Lead Auditor examination offered by the Global Skill Development Council. Other bodies — PECB, BSI and others — run their own lead auditor certifications against the same standard, and the underlying body of knowledge is largely common to all of them, so the material below transfers. What differs between them is the examination format and the post-exam requirements. Hacky Security is not accredited by GSDC or by any other certification body; this is our own preparation course and the exam is taken directly with the body that awards it.

Two standards sit behind the syllabus and it is worth separating them at the outset. ISO/IEC 27001:2022 defines what an information security management system must contain and lists the Annex A controls an organisation selects from. ISO 19011 defines how a management system audit is planned, conducted, reported and followed up, and how auditor competence is judged. A lead auditor is examined on both: the requirements you are auditing against, and the discipline you are auditing with.

Lead auditing is an evidence discipline before it is a security discipline. The recurring question in the classroom is not whether a control is good, but whether what you have in front of you is sufficient objective evidence to raise a finding you could defend to the organisation, to your certification body, and to the next auditor who reads your report.

Module 01 — ISO/IEC 27001:2022 and the ISMS Framework

The standard itself, its structure, and what an information security management system is for.

- The ISO/IEC 27000 family and how the standards in it relate to one another
- The purpose of an ISMS and what distinguishes a management system from a set of controls
- The harmonised high-level structure shared across ISO management system standards
- The 2022 revision and what changed from the 2013 edition, in both the clauses and Annex A
- Amendment 1:2024 and the climate change consideration added to the context clauses
- Terms and definitions that carry precise meaning in audit: conformity, nonconformity, objective evidence, audit criteria
- Certification, accreditation and attestation, and why the three are routinely confused
- The relationship between ISO/IEC 27001 and the guidance in ISO/IEC 27002

Module 02 — Clauses 4 to 10: Management System Requirements

The auditable requirements. Every clause here is a clause you will be asked to gather evidence against.

- Clause 4, context of the organisation: internal and external issues, interested parties and their requirements, and the scope statement
- Clause 5, leadership: top management commitment, the information security policy, and assignment of roles, responsibilities and authorities
- Clause 6, planning: actions to address risks and opportunities, information security objectives, and planning of changes
- Clause 7, support: resources, competence, awareness, communication and documented information

- Clause 8, operation: operational planning and control, risk assessment and risk treatment as performed rather than as documented
- Clause 9, performance evaluation: monitoring and measurement, internal audit and management review
- Clause 10, improvement: nonconformity, corrective action and continual improvement
- Reading a clause as an auditor: separating what is required from what is merely common practice
- Identifying which documented information the standard explicitly requires to be retained

Module 03 — Annex A Controls and the Statement of Applicability

The control set, how an organisation selects from it, and how an auditor tests the selection.

- The structure of Annex A in the 2022 revision and its four control themes
- Organisational controls and the governance evidence that supports them
- People controls, from screening through to responsibilities after employment ends
- Physical controls and what a site walk should actually look for
- Technological controls, including access control, cryptography, logging, and secure development
- Control attributes and how they are used to filter and group the control set
- The Statement of Applicability: justification for inclusion, justification for exclusion, and implementation status
- Testing whether an exclusion is defensible or is simply a control the organisation would rather not implement
- Tracing a control from the risk that justified it to the evidence that it operates

Module 04 — Information Security Risk Management

Risk is the hinge of the whole standard, and the part of an ISMS most often documented rather than performed.

- The risk assessment process the standard requires, and the freedom it leaves on method
- Risk criteria, risk acceptance criteria, and who is entitled to set them
- Identifying information security risks, and the asset, threat and vulnerability framing
- Risk analysis and evaluation, and the difference between a consistent method and a defensible one
- Risk treatment options, and the residual risk that remains after treatment
- Risk owners, risk acceptance and the authority required to sign it off
- The risk treatment plan, and its relationship to the Statement of Applicability
- Auditing risk management: whether the process was run, or a spreadsheet was inherited
- Alignment with the guidance in ISO/IEC 27005 and in ISO 31000

Module 05 — Principles of Auditing

ISO 19011 clause 4. Seven principles that decide whether an audit means anything.

- Integrity, and the professional conduct expected of an auditor
- Fair presentation: reporting truthfully and accurately, including unresolved disagreements
- Due professional care and the judgement expected in every audit situation
- Confidentiality and the handling of information obtained during an audit
- Independence, the basis of impartiality, and the conflicts that compromise it
- Evidence-based approach, and sampling as the rational basis for a reliable conclusion
- Risk-based approach, and directing audit effort at what matters to the organisation
- Applying the principles in practice when the client is also the person paying

Module 06 — Managing an Audit Programme

ISO 19011 clause 5. The programme above the individual audit, and the lead auditor's part in it.

- Establishing audit programme objectives and what drives them
- Determining and evaluating audit programme risks and opportunities
- Roles and responsibilities of the person managing the programme
- Competence requirements for the programme manager and for the audit team
- Establishing the extent of the programme: scope, frequency, methods and resources
- Selecting audit methods, including remote and on-site techniques and their limitations
- Selecting audit team members and assigning responsibility for individual audits
- Managing and retaining audit programme records
- Monitoring, reviewing and improving the programme over time

Module 07 — Conducting an Audit

ISO 19011 clause 6. The audit itself, from initiation to the closing meeting.

- Initiating the audit: establishing contact and determining feasibility
- Preparing audit activities: reviewing documented information, planning, work assignment and preparing working documents
- The audit plan, and negotiating it with the auditee without surrendering scope
- Conducting the opening meeting and setting expectations for the days that follow
- Communication during the audit, including escalation when access or evidence is being withheld
- Collecting and verifying information: interviewing, observing, sampling and reviewing records
- Audit trails, and following one from a claim to the record that supports or contradicts it
- Generating audit findings and determining audit conclusions
- Conducting the closing meeting, and presenting findings that will not be relitigated afterwards

Module 08 — Audit Evidence, Findings and Nonconformity

Where most lead auditor exams are won or lost: turning what you saw into something defensible.

- Objective evidence, and what does not qualify as it
- Sampling approaches, sample size, and stating the basis of your sample in the report
- Writing a finding: the requirement, the evidence, and the statement of nonconformity
- Grading findings, and the distinction between a major and a minor nonconformity
- Opportunities for improvement and observations, and the discipline of not disguising a nonconformity as one
- Nonconformities against a clause compared with nonconformities against the organisation's own documented process
- Handling disagreement over a finding at the closing meeting
- Common errors: findings written as recommendations, evidence written as opinion, and conclusions the evidence does not support

Module 09 — Reporting, Follow-up and Corrective Action

What happens after the closing meeting, which is where an audit either produces change or produces a file.

- Preparing and distributing the audit report, and what it must contain
- Report ownership, retention and confidentiality

- Completing the audit, and the point at which the audit team's responsibility ends
- Conducting audit follow-up, and verifying action rather than accepting a response
- Root cause analysis as the auditee's obligation and the auditor's test of it
- Correction against corrective action, and why accepting the first as the second is the most common audit failure
- Evaluating the effectiveness of corrective action taken
- Closing nonconformities, and the evidence required to do so
- Follow-up audits and the circumstances that require one

Module 10 — Competence, Certification Audits and the Auditor's Role

ISO 19011 clause 7, and the third-party certification context a lead auditor usually operates in.

- Determining auditor competence, and the knowledge and skills specific to information security auditing
- Establishing evaluation criteria and selecting an appropriate evaluation method
- Maintaining and improving auditor competence over a career
- The behaviour expected of an auditor, and leading a team through a difficult audit
- First-party, second-party and third-party audits, and how the auditor's role differs in each
- The certification audit cycle: stage 1, stage 2, surveillance and recertification
- Requirements placed on certification bodies by ISO/IEC 17021-1, and what they mean for you as an auditor working under one
- Scope of certification, and the disputes that arise from a scope statement written too loosely
- The transition to ISO/IEC 27001:2022 and the audit implications for organisations still carrying 2013-era evidence

Who should take this

Internal auditors, compliance and risk managers, information security managers, and consultants who lead or take part in ISMS audits. It also suits second-party auditors assessing suppliers, and security practitioners who are being asked to prepare their own organisation for a certification audit and would rather understand it from the auditor's side first.

There is no mandatory prerequisite for the GSDC examination, but the course assumes you have read ISO/IEC 27001:2022 and have some working exposure to management systems or information security governance. Prior ISO 27001 foundation-level training and experience in a security, quality or compliance role will make the week considerably more productive.

Bring your own copy of the standard if your organisation holds a licence for it. We teach the requirements and the audit method, but we cannot distribute the text of the standard itself.

The exam

The Certified ISO 27001:2022 Lead Auditor examination is set and awarded by the Global Skill Development Council and is taken directly with them.

- 58 multiple-choice questions
- 120 minutes
- A score of 70 per cent is required to pass
- Delivered online with proctoring
- One complimentary retake is included
- The certification is valid for five years

GSDC states no mandatory prerequisite for the examination, though it recommends prior ISO 27001:2022 training and relevant work experience. The examination is purchased from GSDC; we arrange it on your behalf and send you the details, and you choose your own date.

If your employer requires a lead auditor certificate from a specific body — PECB, BSI, or another — tell us at enrolment. The teaching below covers the common body of knowledge, but examination formats differ, and some bodies impose audit-day logging requirements after the exam before the credential is issued.

How we deliver it

Five days, classroom or online live, or at your office for a private group. The format is workshop-led rather than lecture-led: short teaching blocks on the requirement, then evidence exercises using a running case organisation that carries through the whole week.

You will plan an audit, run opening and closing meetings against a role-played auditee, conduct interviews, sample records, write findings and grade them, and then have your findings challenged by another delegate acting for the organisation. Findings that cannot survive that challenge get rewritten, because that is the skill the exam and the job both test.

Module checkpoints each day and a full-length mock examination under timed conditions on the final afternoon.

Mapped to ISO/IEC 27001:2022 and the audit process defined in ISO 19011, and to the GSDC Certified ISO 27001:2022 Lead Auditor examination. Taught from Hacky Security's own curriculum by instructors who conduct ISMS audits for a living. These are our own preparation courses; we are not accredited by GSDC, PECB or any other certification body, and the certificate is awarded by the examining body rather than by us.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

FROM

₹59,000

per person

INR	₹59,000 per person
USD	\$709 per person
GBP	£559 per person
AED	AED 2,599 per person

Group, corporate and repeat-cohort pricing on request. Prices are reviewed quarterly and exclude the exam voucher.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/hacky-lead-auditor-certification-iso-27001/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 12 September 2026.