PENTESTERRA

ISO/IEC 27001:2022 GAP ASSESSMENT

Would Your ISO 27001 Certification Survive an Audit Today?

Technical gap assessment across all 100 ISO/IEC 27001:2022 controls - the 7 ISMS clauses and all 93 Annex A controls - before the auditor arrives.

IN SHORT

Covers ISMS clauses 4-10 plus all 93 technical, organizational, physical and people controls in Annex A (A.5-A.8) of ISO/IEC 27001:2022. Many technical controls (config, crypto, vulnerability management, network, secure development) can be auto-filled from evidence your scans already collected.

100
ISMS + Annex A controls covered

93
Technical, physical and organizational Annex A controls

Certification
Full readiness before the certification audit

THE SITUATION TODAY

WHO YOU ARE

You're the CISO or quality lead of an organization that needs to obtain or renew ISO/IEC 27001 certification - often required by enterprise clients, tenders, or strategic partners.

WHAT HAPPENED

The certification audit is scheduled, and Annex A controls are only partially documented. Some are current, others date back to the last certification cycle.

WHY IT HURTS

A major nonconformity in audit can push certification back by months, while a client or a tender is waiting on that certificate to sign.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME

You want to know, control by control, what's satisfied, what's partial, and what's missing - with real technical evidence attached to every answer, not an optimistic claim nobody has verified.

THE SOLUTION

Pentesterra's ISO/IEC 27001:2022 Gap Assessment: a structured assessment across every control, with technical controls auto-filled from vulnerability scanning, penetration testing, OSINT and External Exposure monitoring wherever evidence exists.

WHY IT'S DIFFERENT

You're not buying another self-assessment questionnaire, and this isn't a legal opinion. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know - a colleague, a supplier, a competitor. And the gap assessment doesn't stop at a paper checklist: technical controls are auto-filled from evidence already on file, with cross-standard mapping to the other 12 frameworks the platform supports, so a second audit never starts from zero.

CONCRETE PROOF

The result is a complete, ready-to-deliver PDF report covering every control, with a direct reference to the legal/regulatory basis. If gaps come up, we propose the additional services to close them: vulnerability assessment, network or application penetration testing, phishing training and simulation.

WHAT'S ACTUALLY INCLUDED

Not a generic checklist - the real controls of ISO/IEC 27001:2022, grouped the way you'll see them in the platform.

ISMS Clauses 4-10

The 7 management clauses of the information security management system.

- Context, leadership, planning
- ISMS support and operation
- Performance evaluation and continual improvement

Annex A.5 - Organizational Controls (37)

The largest Annex A group: policy, roles, supplier management, incidents.

- Security policy and roles and responsibilities
- Supplier risk management
- Information security incident management

Annex A.6 People (8) + A.7 Physical (14)

Controls on people and physical security.

- Screening, training and awareness of personnel
- Physical access control and secure areas
- Secure disposal of equipment and media

Annex A.8 - Technological Controls (34)

The technical controls auto-filled from vulnerability scans and pentests.

- Technical vulnerability management
- Cryptography and secure configurations
- Secure development and network monitoring

PENTESTERRA

ISO/IEC 27001:2022 GAP ASSESSMENT

WHAT YOU GET

- ✓ An exportable XLSX control matrix, with the status of every individual control
- ✓ An editable DOCX gap report, ready for your auditor or your board
- ✓ Technical controls auto-filled from evidence the platform already collected
- ✓ Guided applicability check by sector, country, and company size
- ✓ Cross-standard mapping to the other 12 frameworks the platform supports - answer once, reuse across standards
- ✓ A one-click auditor package: questionnaire, technical evidence and gap report together
- ✓ Prioritized remediation recommendations for the gaps found

HOW IT WORKS

1

We define the scope

Assessment boundary, systems and processes involved - we set the scope together.

2

We collect the evidence

Technical controls are auto-filled from evidence the platform already collected.

3

We complete the questionnaire

Non-technical controls are verified with your team.

4

We deliver the report

A complete PDF with the gaps found and the actions to take.

Find out how ready you are for ISO/IEC 27001:2022

A complete report, ready to present to clients, auditors, or your board.

Request your ISO/IEC 27001:2022 Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance