isms.online

ISO 27701 AUDIT ROADMAP

ISO 27701 is a privacy extension to ISO 27001, which provides guidelines and requirements for implementing and managing a privacy information management system (PIMS) within an existing Information Security Management System (ISMS).

An ISO 27701 audit verifies whether an organisation has effectively implemented and maintained its PIMS according to the standard's requirements.

HERE ARE FIVE STEPS TO HELP YOU PREPARE FOR AN ISO 27701 AUDIT:

1

ESTABLISH CLEAR TIMELINES, BUDGETS AND RESPONSIBILITIES

To effectively plan a budget and project timeline for an audit project, it is essential to determine the following:

- The scope of the audit
- Identify team members with the required skills
- Create a project plan that outlines timelines, tasks, and responsibilities.

Estimating the required budget, allocating resources, monitoring progress, and communicating effectively with stakeholders are also critical for achieving a successful outcome. Regular review and updating of the audit plan is essential for ensuring continued effectiveness.

2

REVIEW AND ASSESS YOUR CURRENT DATA PRIVACY LANDSCAPE

Understanding your organisation's data practices, how information flows through your systems, and the processes impacting the data moving through your business is essential. When assessing this, you should include the documentation, policies, procedures, and controls in place to manage privacy information within your organisation.

Once you're clear on how you're managing data privacy in the present, bring in the ISO 27701 controls to map:

- Where you already meet specific controls
- Areas where you need to do additional work to meet controls
- New processes for controls you're not currently addressing
- The requirements for additional controls added as part of the ISO 27001 2022 update. You can find more about the 2022 update on our website.

3

DEVELOP AND IMPLEMENT A ROADMAP TO COMPLIANCE

Once you've reviewed your current data privacy landscape and mapped the ISO 27701 controls, it's time to create a plan to address the data privacy gaps, update existing processes that do not meet minimum standards and document your processes.

Key processes to consider here are:

- Updating or creating your record of processing activity (ROPA)
- Conducting data privacy impact assessments (DPIA) against each of your identified processes
- Developing your privacy policy
- Establishing your 'Data Subject Rights' management process
- A clear incident management plan, including notification processes and regulatory requirements
- Vendor management, ensuring your suppliers and the wider supply chain meet your minimum standards

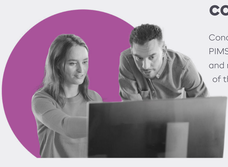
4

TRAINING AND ENGAGEMENT

Everyone within your organisation must be involved in the audit process to ensure the work building your PIMS benefits your business long term. This can be achieved by ensuring you provide training to all employees relevant to their roles and use of data.

Training should include the requirements of the ISO 27701 standard, the organisation's policies and procedures contextualised for the different business units within your organisation, and clearly highlight the importance of maintaining confidentiality and privacy. Overly generalised training will not engage your people with the process and therefore fail to embed a culture of privacy.

5



CONDUCT AN INTERNAL AUDIT REVIEW

Conduct a thorough internal audit of your PIMS to ensure it functions as intended and meets all the mandatory requirements of the ISO 27701 standard. Doing so will enable you to identify areas where further improvements might be needed or processes that need clarification to ensure compliance before your certification audit.

An internal audit will also enhance confidence in your PIMS, demonstrate your privacy commitment to external stakeholders and, more importantly, help you plan and streamline the certification audit process by identifying areas and topics that may be raised by your auditor and putting in place processes, reasoning and clarifications ahead of time.

By following these steps, you can ensure that your organisation is prepared for an ISO 27701 audit and that your PIMS effectively manages privacy information in compliance with the standard's requirements.

UNLOCK YOUR COMPETITIVE ADVANTAGE TODAY

If you want to achieve compliance with ISO 27001 or ISO 27701, you can start your journey to better information and data privacy security with ISMS.online.

isms.online