# ISO 27001 Scope

## What should be in the scope of an ISO 27001 Audit?

The tricky thing with an ISMS audit is that the Audit Scope is defined in consultation with the entity up front so there is not a specific list you can refer to.

The audit scope provided to you by your auditor should describe the range and limits of the audit for example the locations, the organisations business units, the activities, the systems and the processes as well as the time period covered by the audit.

Taking into account the limited duration of the audit the auditor determines which business units and processes systems they will audit. It is critical the audit scope chosen by the auditors be representative of the management system in scope.

As part of the ISO 27001 audit engagement your auditor should have put together a detailed plan to determine the scope and the materiality of certain parts of scope.  Materiality will help define what processes they will place emphasis on during the on-site/evidence collection part of the audit.  The auditor will then adjust their sampling plan based on the materiality of each processor asset.

In summary make sure your assets are well documented and assign them materiality rating, based on risk, then look to work with your auditor to develop a detailed audit plan based on that asset list.

# The Scope Statement

A Scope Statement is required if you intend to get ISO 27001 certification.

## Sample scope statement

The scope encompasses all (Company Name) employees, (Company Name) locations, (Company Name) owned technology and data assets and (Company Name) businesses processes that deliver:

* (List all product and services in scope).

Tip: Carefully consider which of the backend systems you wish to include. The most important systems to include is the parts that are important to your customers.

You may wish to articulate very clearly what is in scope vs out of scope. Here is an example of a scope statement clearly articulated.

## Product and Services

The following products and services are in scope:

#### In Scope

* Product 1
* Service 1
* Service 2

#### Out of Scope

Tip: Consider excluding back office systems that support the operation of the business that do not directly support in-scope products and services.

* HR System 1
* Marketing System 1
* Auditing st

## Locations

#### In Scope

The following locations are in scope:

Tip: List all locations in scope. Consider defining the floor and shared offices

* Office 1, Building name, Address
* Office 2, Building name, Address

#### Out of Scope

The following locations are out of scope:

Tip: List all locations out of scope. Consider defining the third party locations such as data centres and shared offices.

* Third party locations such as data centres
* Office 5, Building name, Address

## Business Units/Teams/People

#### In Scope

The following company employees deliver the in scope product and services:

Tip: List all teams that support the in-scope product and services.

* Technology Team, Sydney
* Consultants, Sydney and Melbourne

#### Out of Scope

The following company employees do not deliver the in scope product and services

Tip: List all teams that do not support the in-scope product and services.

* Finance Team in Brisbane

## Technology

Tip: Provide an overview, in words, of the technology that supports the in-scope products and services.

What is it called? What does it do? What does it connect with? What is the boundary?

Provide a current architecture diagram with document control and last reviewed date.

Technology overview

### Network

Tip: Provide the most recent up to date network diagrams with document control and last reviewed date.

Network diagram/links to documents