

ISO 27001:2022

SCOPING GUIDE



ISO 27001:2022 Scoping Guide

SI No	Questions	Response
Organization		
1	What are the main business lines of the organization	
2	What are the services offered by the organization to it's customers	
3	Who are the customers of the organization	
4	What are the domains/fields the organization is catering to	
5	What are the locations that the organization is operation from	
6	what are the geographical locations that the organization is catering to	
7	What are the response for the organization to undergo ISO 27001 certification	
8	What is the structure of the organization (Org Chart)	
9	What are business verticals of the organization	
10	What are the various business departments within the organization	
11	What are the processes that deal with critical/sensitive data of the organization	
12	What are the systems that are involved in transmission, storage and processing of critical/sensitive data of the organization	
13	What are the applications that are developed in house that are involved in transmission, storage and processing of critical/sensitive data of the organization	
14	What are the third party applications that are involved in transmission, storage and processing of critical/sensitive data of the organization	
Business Units		
15	What is the functions of this Business Unit	
16	What are their roles and responsibility	
17	What are the other teams which are dependent on this business unit	
18	What are the other teams which you are dependant on	
19	What roles of the business unit has access to critical/sensitive data of the organization	
20	What roles of the business unit is involved in transmission, storage and processing of critical/sensitive data of the organization	
21	What kind processes are involved in the business unit	

22	What are the processes that is involved in transmission, storage and processing of critical/sensitive data of the organization	
23	For each operation understand the data flow	
24	What are the upstream and downstream applications involved	
25	How are they accessing the data - on site or remote access	
26	Understand if there are any third party who is involved in this process	
27	If yes, who are the third parties who are involved in transmission, storage and processing of critical/sensitive data of the organization	
Applications		
28	What is the application used for	
29	What kind of application is it, is it a SAAS or On Prem	
30	Is it procured or developed in house	
31	Understand how the application works	
32	Is the application involved in transmission, storage and processing of critical/sensitive data of the organization	
33	What is the role of the application in transmission, storage and processing of critical/sensitive data of the organization	
34	What are the upstream and downstream applications involved	
35	What all systems are connected to the application	
36	Dependant systems for each application	
37	Who all have access to the application	
Questions from Clauses		
38	What are the internal issues that are relevant to the organization	
39	What are the external issues that are relevant to the organization	
40	What the processes in which internal or external issues are identified	
41	What the applications in which internal or external issues are identified	
42	Who are the interested parties relevant to the organization	
43	What are the needs and expectations of the interested parties	
44	What are the processes that are affected by the needs and expectations of the interested parties	
45	What are the applications that are affected by the needs and expectations of the interested parties	
ISMS Scope Finalization		
46	From the responses for the above questions determine:	
47	The Main Departments for the Scope of ISMS	

48	The Interfacing Departments for the Scope of ISMS	
49	The Interfaces and Dependencies for the Scope of ISMS	
50	The Locations for the Scope of ISMS	
51	The Processes for the Scope of ISMS	
52	The Systems for the Scope of ISMS	
53	The Applications for the Scope of ISMS	
54	Define and establish the boundaries and applicability of ISMS	
55	All the Locations, Departments, Processes, systems and applications that are excluded from the Scope of ISMS	

Finally, Draft a scope statement for ISO 27001:2022 and prepare scope document

**FOLLOW US ON
LINKEDIN FOR MORE FREE
CHECKLISTS**

**PLAYBOOK
MADE WITH**

