Checklist obligatory requirements for implementation of ISO/IEC 27001:2013

Please fill out the following form completely to determine the maturity of your ISO/IEC 27001:2013 implementation and send it back to us.

Based on your answers and a personal meeting we will create an appropriate and detailed offer for your company.

	Obligatory requirements	Sections according to ISO 27001:2013	Available?	If yes – where? If no – why not?
1.	Is the **scope of the ISMS** determined and documented?	4.3		
2.	Is the **information security policy** aligned and documented?	5.2		
3.	Is the **information security risk assessment** process defined?	6.1.2		
4.	Is the **Statement of Applicability** (SoA) documented?	6.1.3 d)		
5.	Are the **information security risk treatment plan** and the **results of the risk treatment** documented?	6.1.3 e) and 8.3		
6.	Are the **information security objectives** (at relevant functions and levels) aligned and documented?	6.2		
7.	Are appropriate **documented information of competences** retained?	7.2		
8.	Are documented information of the results of the **information security risk assessments** retained?	8.2		
9.	Is the **information security performance** (and the effectiveness of the ISMS) evaluated?	9.1		
10.	Is the **internal audit program** available and documented?	9.2		
11.	Are the **results of the internal audits** documented?	9.2		
12.	Are the **results of the management reviews** available?	9.3		
13.	Are **results of corrective actions** available?	10.1		
14.	Are the **responsibilities and controls** for information security defined?	A.7.2.1		
15.	Is an **inventory of assets** available?	A.8.1.1		
16.	Are rules for the **acceptable use of assets** documented?	A.8.1.3		

	Obligatory requirements	Sections according to ISO 27001:2013	Available?	If yes – where? If no – why not?
17.	Is an **access control policy** documented and communicated?	A.9.1.1		
18.	Is the **policy on the use of cryptographic controls** developed and implemented?	A 10.1.1		
19.	Are **operating procedures** (IT, e.g. for change management, backup or patch management etc.) documented and available for all users who need them?	A.12.1.1		
20.	Are the **logs of events, exceptions and system administration and operator activities** documented?	A.12.4.1 und A.12.4.3		
21.	Are the requirements for **confidentiality and non-disclosure agreements** documented?	A.13.2.4		
22.	Are **secure system engineering principles** established?	A.14.2.5		
23.	Is an **information security policy for suppliers** documented and communicated?	A.15.1.1		
24.	Is the process for **information security incidents** defined?	A.16.1.5		
25.	Is the process for **information security continuity** established?	A.17.1.2		
26.	Are all relevant **legislative statutory, regulatory and contractual requirements** identified and complied with?	A.18.1.1		

Please do not hesitate to contact us if you have any questions or need further information.

We are looking forward to your request!

Your OPTIMAbit-Experts-Team