# Appendix 3 – Internal Audit Checklist for ISO 27001 and ISO 22301

### 1. Internal audit checklist for ISO 27001

Clause	Requirement of the standard	Compliant	Evidence
		Yes/No	
4.2	Did the organization determine interested		
	parties?		
4.2	Does the list of all of interested parties'		
	requirements exist?		
4.3	Is the scope documented with clearly		
	defined boundaries and interfaces?		
5.1	Are the general ISMS objectives compatible		
	with the strategic direction?		
	The second second second second		

#### Appendix 3 – Internal Audit Checklist

ver [version] from [date]

Page **1** of **13** 

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

### Commented [270011]: To learn more about this topic:

- $\bullet$  read this article: How to make an Internal Audit checklist for ISO 27001 / ISO 22301
- https://advisera.com/27001academy/knowledgebase/how-to-make-an-internal-audit-checklist-for-iso-27001-iso-22301/
- consider taking this free online training: ISO 27001 Internal Auditor Course <a href="https://training.advisera.com/course/iso-27001-internal-auditor-course/">https://training.advisera.com/course/iso-27001-internal-auditor-course/</a>
- take a look at this book: ISO Internal Audit: A Plain English Guide https://advisera.com/books/iso-internal-audit-plain-english-guide/

#### Commented [270012]:

#### Commented [270014]:

Commented [270013]: To be filled in during the audit – fill in Yes or No depending on whether the company is compliant or not.

7.1	Are adequate resources provided for all the elements of ISMS?
7.2	Are required competences defined, trainings performed, and records of competences maintained?
	Statement of the later of the l
	To the second section of
	The state of the s
	The control of the co
9.3	Did management decide on all the crucial issues important for the success of the ISMS?
10.1	Does the organization react to every nonconformity?
10.1	Does the organization consider eliminating the cause of nonconformity and, where

ver [version] from [date]

Page **2** of **13** 

[organization name]

ver [version] from [date]

Page **3** of **13** 

[confidentiality level]

[organization name] [confidentiality level]

A.5.13	Is the classified information la according to the defined proce		
M.J.13	Is the protection of information		
	regulated in formal policies an		
A.5.14	procedures?		
	nternal Audit Checklist ver [ve	rsion] from [date]	Page 4 of 1

Appendix 3 – Internal Audit Checklist

ver [version] from [date]

Page **4** of **13** 

ver [version] from [date]

Page **5** of **13** 

	Is information security regularly reviewed	
A.5.35	by an independent auditor?	
	Are delivery and leading areas controlled in	
	Are delivery and loading areas controlled in	
. 7.0	such a way that unauthorized persons	
A.7.2	cannot enter the company premises?	

ver [version] from [date]

Page **6** of **13** 

	Are secure areas located in such a way that	
A.7.3	they are not visible to outsiders, and not easily reached from the outside?	
	Are premises monitored for unauthorized	
A.7.4	access?  Are the alarms, fire protection, and other	
A.7.5	systems installed?	
	Is the access to source code restricted to	
A.8.4	authorized persons?	Dags 7 of 12

ver [version] from [date]

Page **7** of **13** 

[organization name] [confidentiality level]

	Is secure log-on required on systems
A.8.5	according to the Access control policy?
	Does someone monitor the use of
	resources and forecast the required
A.8.6	capacity?
	Is anti-virus software, and other software
	for malware protection, installed and
A.8.7	updated?
	Control of the Contro
	the distance on the other state.
	the same of the sa
•	No college de la
	Service del relación colaborar.
	Statement and the second second
	THE RESERVE AND ADDRESS OF THE PARTY OF THE
	and the same of th
	The same of the sa
	and the second second
	The state of the s
	Carrier and
	application and the same about
	Contraction Street, Contraction
	Charles and Artist Charles
	Street and the second party of the second
	Control of the second
•	TTTT
	The second secon
	Carlotte Street Street
	and the same of th
	production of the control of the con
	to make your or species
	representation of the agreement control
	Marin Control (Marin Marin)

Appendix 3 – Internal Audit Checklist

ver [version] from [date]

Page **8** of **13** 

[organization name] [confidentiality level]

	Are clocks on all IT systems synchronized	
A.8.17	with a single source of correct time?	
	Is the use of utility tools that can override	
	the security controls of applications and	
	systems strictly controlled and limited to a	
A.8.18	narrow circle of employees?	
	Are secure coding principles applied into	i i
A.8.28	software development?	
	Is testing for proper implementation of	
	security requirements performed during	
A.8.29	the software development?	
	Are the criteria for accepting the systems	
A.8.29	defined?	
	Is the outsourced development of systems	
A.8.30	monitored?	
	Are development, testing, and production	
A.8.31	environments strictly separated?	
	Are all the changes to IT systems, but also	
	to other processes that could affect	
A.8.32	information security, strictly controlled	
	ntornal Audit Charlelist	1 Dans 0 of 12

Appendix 3 – Internal Audit Checklist

ver [version] from [date]

Page **9** of **13** 

# 2. Internal audit checklist for ISO 22301

Clause	Requirement of the standard	Compliant Yes/No	Evidence	
4.2.1	Did the organization determine interested	resyrto		
4.2.2	parties?  Does the list of all of interested parties'			
	requirements exist?			
4.2.2	Did the organization determine a process to			
	handle applicable and regulatory requirements?			
5.3	Are the necessary changes for the BCMS carried			
	out in a planned manner?			
7.1	Are adequate resources provided for all the			
	elements of the BCMS?			

ver [version] from [date]

Appendix 3 – Internal Audit Checklist

Page **11** of **13** 

©2022 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.

Commented [270015]:

Commented [270017]: To be filled in during the audit –

Commented [270016]: To be filled in during the audit – fill in Yes or No depending on whether the company is compliant or not.

performed, and records of competences maintained?	
maintained?	
	1
.1 Do the business continuity procedures or plans	
have these elements: have specific steps, are	
flexible for all kinds of disruption conditions, and	
are focused on minimizing the consequences,	
assign roles and responsibilities?	
Do incident response procedures exist with	
initiation thresholds and procedures of response?	
.3 Does a procedure exist for communicating with	Page 12 of 13

ver [version] from [date]

Page **12** of **13** 

	interested parties, which defines how the means of communication will be available?	
8.4.4	Do business continuity plans exist that include roles and responsibilities and detailed steps for the recovery of activities?	
	and the same of th	
9.3	Did management decide on all the crucial issues	
10.1	important for the success of the BCMS?  Does the organization react to every	
	nonconformity?	
10.1	Does the organization consider eliminating the	
	cause of nonconformity and, where appropriate, take corrective action?	
10.1	Are all nonconformities recorded, together with	
	corrective actions?	

ver [version] from [date]

Page **13** of **13**