

ISO 27001-2013 Auditor Checklist

01/02/2018

The ISO 27001 Auditor Checklist gives you a high-level overview of how well the organisation complies with ISO 27001:2013.

The checklist details specific compliance items, their status, and helpful references.

Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Control	Description	Applicable	In Compliance	References	Issues
5	Information security policies				
5.1	Management direction for information security				
5.1.1	Policies for information security	Yes	Yes	Information Security Policies and Procedures	
5.1.2	Review of the policies for information security	Yes	Yes	Information Security Policies and Procedures - Review; ISO 27001 Compliance Questionnaire - Information Security Policy; Evidence of Compliance - Information Security Policies	
6	Organization of information security				
6.1	Internal organization				
6.1.1	Information security roles and responsibilities	Yes	Yes	Information Security Policies and Procedures - Security Roles and Responsibilities	
6.1.2	Segregation of duties	Yes	Yes	Information Security Policies and Procedures - Security Roles and Responsibilities	
6.1.3	Contact with authorities	No	No	Information Security Policies and Procedures - Contact with Authorities; ISO 27001 Compliance Questionnaire - Contact with authorities; Evidence of Compliance - Organisation of Information Security	See Risk Treatment Plan
6.1.4	Contact with special interest groups	No	No	Information Security Policies and Procedures - Contact with special interest groups; ISO 27001 Compliance Questionnaire - Contact with special interest groups; Evidence of Compliance - Organisation of Information Security	See Risk Treatment Plan
6.1.5	Information security in project management	No	No	Information Security Policies and Procedures - Information security in project management; ISO 27001 Compliance Questionnaire - Information security in project management; Evidence of Compliance - Organisation of Information Security	See Risk Treatment Plan
6.2	Mobile devices and teleworking				
6.2.1	Mobile device policy	Yes	Yes	Information Security Policies and Procedures - Mobile Device Policy; ISO 27001 Compliance Questionnaire - Mobile Device and Teleworking; Evidence of Compliance - Organisation of Information Security	

ISO 27001-2013 Auditor Checklist

01/02/2018

The ISO 27001 Auditor Checklist gives you a high-level overview of how well the organisation complies with ISO 27001:2013.

The checklist details specific compliance items, their status, and helpful references.

Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Control	Description	Applicable	In Compliance	References	Issues
6.2.2	Teleworking	Yes	Yes	Information Security Policies and Procedures - Teleworking; ISO 27001 Compliance Questionnaire - Mobile Device and Teleworking; Evidence of Compliance - Organisation of Information Security	
A.7 Human resource security					
7.1	Prior to employment				
7.1.1	Screening	Yes	Yes	Information Security Policies and Procedures - Human Resource Security; ISO 27001 Compliance Questionnaire - Human Resource Security	
7.1.2	Terms and conditions of employment	Yes	Yes	Information Security Policies and Procedures - Human Resource Security; ISO 27001 Compliance Questionnaire - Human Resource Security	
7.2	During employment				
7.2.1	Management responsibilities	Yes	Yes	Information Security Policies and Procedures - Human Resource Security	
7.2.2	Information security awareness, education, and training	No	No	Information Security Policies and Procedures - Information Security Awareness and Training; ISO 27001 Compliance Questionnaire - Information Security Awareness and Training	See Risk Treatment Plan
7.2.3	Disciplinary process	Yes	Yes	Information Security Policies and Procedures - Human Resource Security	
7.3	Termination and change of employment				
7.3.1	Termination or change of employment responsibilities	Yes	Yes	Information Security Policies and Procedures - Human Resource Security	
A.8 Asset management					
8.1	Responsibilities for assets				
8.1.1	Inventory of assets	Yes	Yes	Asset Inventory Worksheet	
8.1.2	Ownership of assets	Yes	Yes	Asset Inventory Worksheet	
8.1.3	Acceptable use of assets	Yes	Yes	Information Security Policies and Procedures - Asset Management	
8.1.4	Return of assets	Yes	Yes	Information Security Policies and Procedures - Asset Management; ISO 27001 Compliance Questionnaire - Employee Termination	
8.2	Information classification				

ISO 27001-2013 Auditor Checklist

01/02/2018

The ISO 27001 Auditor Checklist gives you a high-level overview of how well the organisation complies with ISO 27001:2013.

The checklist details specific compliance items, their status, and helpful references.

Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Control	Description	Applicable	In Compliance	References	Issues
8.2.1	Classification of information	Yes	Yes	Information Security Policies and Procedures - Information Classification and Labeling	
8.2.2	Labeling of information	No	No	Information Security Policies and Procedures - Information Classification and Labeling; ISO 27001 Compliance Questionnaire - Information Classification and Labeling	See Risk Treatment Plan
8.2.3	Handling of assets	Yes	Yes	Information Security Policies and Procedures - Information Classification and Labeling	
8.3	Media handling				
8.3.1	Management of removable media	No	No	Information Security Policies and Procedures - Management of removable media; Site Walkthrough Checklist	See Risk Treatment Plan
8.3.2	Disposal of media	No	No	Information Security Policies and Procedures - Management of removable media; Site Walkthrough Checklist	See Risk Treatment Plan
8.3.3	Physical media transfer	Yes	Yes	Information Security Policies and Procedures - Management of removable media; ISO 27001 Compliance Questionnaire - Media Handling	
A.9	Access control				
A.9	Responsibilities for assets				
9.1.1	Access control policy	Yes	Yes	Information Security Policies and Procedures - Access control policy; Evidence of Compliance - User Access	
9.1.2	Access to networks and network services	Yes	Yes	Information Security Policies and Procedures - Access control policy; Evidence of Compliance - User Access	
9.2	Responsibilities for assets				
9.2.1	User registration and de-registration	Yes	Yes	Information Security Policies and Procedures - Access control policy; Evidence of Compliance - User Access	
9.2.2	User access provisioning	Yes	Yes	Information Security Policies and Procedures - Access control policy; Evidence of Compliance - User Access	
9.2.3	Management of privileged access rights	Yes	Yes	Information Security Policies and Procedures - Access control policy; Evidence of Compliance - User Access	

ISO 27001-2013 Auditor Checklist

01/02/2018

The ISO 27001 Auditor Checklist gives you a high-level overview of how well the organisation complies with ISO 27001:2013.

The checklist details specific compliance items, their status, and helpful references.

Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Control	Description	Applicable	In Compliance	References	Issues
9.2.4	Management of secret authentication information of users	Yes	Yes	Information Security Policies and Procedures - Access control policy; Evidence of Compliance - User Access	
9.2.5	Review of user access rights	No	No	Information Security Policies and Procedures - Access control policy; User Access Rights Review Worksheet; Evidence of Compliance - User Access Management	See Risk Treatment Plan
9.2.6	Removal or adjustment of access rights	Yes	Yes	Information Security Policies and Procedures - Access control policy; Evidence of Compliance - User Access	
9.3	User responsibilities				
9.3.1	Use of secret authentication information	Yes	Yes	Information Security Policies and Procedures - User responsibilities	
9.4	System and application access control				
9.4.1	Information access restrictions	No	No	Information Security Policies and Procedures - Access Control Policy; Evidence of Compliance - User access management	See Risk Treatment Plan
9.4.2	Secure log-on procedures	Yes	Yes	Information Security Policies and Procedures - Access Control Policy; Evidence of Compliance - User access management	
9.4.3	Password management system	No	No	Information Security Policies and Procedures - Access Control Policy; Evidence of Compliance - User access management	See Risk Treatment Plan
9.4.4	Use of privileged utility programs	No	No	Information Security Policies and Procedures - Access Control Policy; Evidence of Compliance - User access management	See Risk Treatment Plan
9.4.5	Access control to program source code	No	No	Information Security Policies and Procedures - Access Control Policy; ISO 27001 Compliance Questionnaire - Access control to program source; Evidence of Compliance - User access management	See Risk Treatment Plan
A.10	Cryptography				
10.1	Cryptographic controls				

ISO 27001-2013 Auditor Checklist

01/02/2018

The ISO 27001 Auditor Checklist gives you a high-level overview of how well the organisation complies with ISO 27001:2013.

The checklist details specific compliance items, their status, and helpful references.

Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Control	Description	Applicable	In Compliance	References	Issues
10.1.1	Policy on the use of cryptographic controls	No	No	Information Security Policies and Procedures - Cryptography; ISO 27001 Compliance Questionnaire - Cryptography; Evidence of Compliance - Cryptography	See Risk Treatment Plan
10.1.2	Key management	No	No	Information Security Policies and Procedures - Cryptography; ISO 27001 Compliance Questionnaire - Cryptography; Evidence of Compliance - Cryptography	See Risk Treatment Plan
A.11 Physical and environmental security					
11.1 Secure areas					
11.1.1	Physical security perimeter	No	No	Information Security Policies and Procedures - Physical and environmental security; Site Walkthrough Checklist	See Risk Treatment Plan
11.1.2	Physical entry controls	No	No	Information Security Policies and Procedures - Physical and environmental security; Site Walkthrough Checklist	See Risk Treatment Plan
11.1.3	Securing offices, rooms and facilities	No	No	Information Security Policies and Procedures - Physical and environmental security; Site Walkthrough Checklist	See Risk Treatment Plan
11.1.4	Protection against external and environmental threats	Yes	Yes	Information Security Policies and Procedures - Physical and environmental security	
11.1.5	Working in secure areas	Yes	Yes	Information Security Policies and Procedures - Physical and environmental security	
11.1.6	Delivery and loading areas	Yes	Yes	Information Security Policies and Procedures - Physical and environmental security	
11.2 Equipment					
11.2.1	Equipment siting and protection	Yes	Yes	Information Security Policies and Procedures - Physical and environmental security; Site Walkthrough Checklist	
11.2.2	Supporting utilities	Yes	Yes	Information Security Policies and Procedures - Physical and environmental security	
11.2.3	Cabling security	No	No	Information Security Policies and Procedures - Physical and environmental security; Site Walkthrough Checklist	See Risk Treatment Plan
11.2.4	Equipment maintenance	Yes	Yes	Information Security Policies and Procedures - Physical and environmental security	

ISO 27001-2013 Auditor Checklist

01/02/2018

The ISO 27001 Auditor Checklist gives you a high-level overview of how well the organisation complies with ISO 27001:2013.

The checklist details specific compliance items, their status, and helpful references.

Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Control	Description	Applicable	In Compliance	References	Issues
11.2.5	Removal of assets	Yes	Yes	Information Security Policies and Procedures - Physical and environmental security	
11.2.6	Security of equipment and assets off-premises	Yes	Yes	Information Security Policies and Procedures - Physical and environmental security	
11.2.7	Secure disposal or re-use of equipment	Yes	Yes	Information Security Policies and Procedures - Physical and environmental security	
11.2.8	Unattended user equipment	No	No	Information Security Policies and Procedures - Physical and environmental security; Evidence of Compliance - Screen Lock Settings	See Risk Treatment Plan
11.2.9	Clear desk and clear screen policy	No	No	Information Security Policies and Procedures - Physical and environmental security; Evidence of Compliance - Screen Lock Settings; Site Walkthrough Checklist	See Risk Treatment Plan
A.12 Operations security					
12.1	Operational procedures and responsibilities				
12.1.1	Documented operating procedures	Yes	Yes	Information Security Policies and Procedures - Documented operating procedures; ISO 27001 Compliance Questionnaire - Documented operating procedures	
12.1.2	Change management	Yes	Yes	Information Security Policies and Procedures - Documented operating procedures	
12.1.3	Capacity management	Yes	Yes	Information Security Policies and Procedures - Documented operating procedures	
12.1.4	Separation of development, testing and operational environments	Yes	Yes	Information Security Policies and Procedures - Documented operating procedures; Asset inventory worksheet	
12.2	Protection from malware				
12.2.1	Controls against malware	No	No	Information Security Policies and Procedures - Protection from malware; Evidence of Compliance - Endpoint Security	See Risk Treatment Plan
12.3	Backup				
12.3.1	Information Backup	Yes	Yes	Information Security Policies and Procedures - Backup; Evidence of Compliance - Backup	
12.4	Logging and Monitoring				

ISO 27001-2013 Auditor Checklist

01/02/2018

The ISO 27001 Auditor Checklist gives you a high-level overview of how well the organisation complies with ISO 27001:2013.

The checklist details specific compliance items, their status, and helpful references.

Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Control	Description	Applicable	In Compliance	References	Issues
12.4.1	Event logging	No	No	Information Security Policies and Procedures - Logging and monitoring; Evidence of Compliance - Logging and monitoring; Login History Reports	See Risk Treatment Plan
12.4.2	Protection of log information	No	No	Information Security Policies and Procedures - Logging and monitoring; Evidence of Compliance - Logging and monitoring; Login History Reports	See Risk Treatment Plan
12.4.3	Administrator and operator log	No	No	Information Security Policies and Procedures - Logging and monitoring; Evidence of Compliance - Logging and monitoring; Login History Reports	See Risk Treatment Plan
12.4.4	Clock synchronization	No	No	Information Security Policies and Procedures - Logging and monitoring; Evidence of Compliance - Logging and monitoring; Login History Reports	See Risk Treatment Plan
12.5	Control of operational software				
12.5.1	Installation of software on operational systems	Yes	Yes	Information Security Policies and Procedures - Control of operational software	
12.6	Technical vulnerability management				
12.6.1	Management of technical vulnerabilities	No	No	Information Security Policies and Procedures - Technical vulnerability management; Evidence of Compliance - Technical vulnerability management; External Vulnerability Scan summary; Internal Vulnerability Scan summary	See Risk Treatment Plan
12.7.2	Restriction on software installation	No	No	Information Security Policies and Procedures - Technical vulnerability management; Evidence of Compliance - Restriction on software installation	See Risk Treatment Plan
12.7	Information systems audit considerations				
12.7.1	Information system audit control	Yes	Yes	Information Security Policies and Procedures - Information systems audit controls	
A.13	Communications security				
13.1	Network security management				
13.1.1	Network controls	Yes	Yes	Information Security Policies and Procedures - Network controls	
13.1.2	Security of network services	Yes	Yes	Information Security Policies and Procedures - Security of network services	

ISO 27001-2013 Auditor Checklist

01/02/2018

The ISO 27001 Auditor Checklist gives you a high-level overview of how well the organisation complies with ISO 27001:2013.

The checklist details specific compliance items, their status, and helpful references.

Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Control	Description	Applicable	In Compliance	References	Issues
13.1.3	Segregation in networks	Yes	Yes	Information Security Policies and Procedures - Segregation in networks; Evidence of Compliance - Segregation in Networks	
13.2	Information transfer				
13.2.1	Information transfer policies and procedures	Yes	Yes	Information Security Policies and Procedures - Information transfer policies	
13.2.2	Agreements on information transfer	No	No	Information Security Policies and Procedures - Agreements on information transfer	See Risk Treatment Plan
13.2.3	Electronic messaging	Yes	Yes	Information Security Policies and Procedures - Electronic messaging	
13.2.4	Confidentiality or non-disclosure agreements	Yes	Yes	Information Security Policies and Procedures - Confidentiality or non-disclosure agreements	
A.14	System acquisition, development and maintenance				
14.1	Security requirements of information systems				
14.1.1	Information security requirements analysis and specification	Yes	Yes	Information Security Policies and Procedures - Information security requirements analysis and requirements	
14.1.2	Securing application services on public networks	Yes	Yes	Information Security Policies and Procedures - Securing application services on public networks; Evidence of Compliance - Application Security on Public Networks	
14.1.3	Protecting application service transactions	Yes	Yes	Availability of information processing facilities	
14.2	Security in development and support processes				
14.2.1	In-house development	Yes	Yes	In-house Development; ISO 27001 Compliance Questionnaire - System acquisition, development and maintenance	
A.15	Suppliers relationships				
A.16	Information security incident management				
16	Information security management	No	No	Information Security Policies and Procedures - Information security incident management; ISO 27001 Compliance Questionnaire - Information security incident management	See Risk Treatment Plan
A.17	Information security aspects of business continuity				

ISO 27001-2013 Auditor Checklist

01/02/2018

The ISO 27001 Auditor Checklist gives you a high-level overview of how well the organisation complies with ISO 27001:2013.

The checklist details specific compliance items, their status, and helpful references.

Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Control	Description	Applicable	In Compliance	References	Issues
17.1	Information security continuity	Yes	Yes	Information Security Policies and Procedures - Business Continuity Plan; ISO 27001 Compliance Questionnaire - Business Continuity Management	
17.2	Redundancies				
A.18	Compliance				
18.1	Compliance with legal and contractual requirements				
18.1.1	Identification of applicable legislation and contractual requirements	Yes	Yes	Information Security Policies and Procedures - Applicable Legislation; ISO 27001 Compliance Questionnaire - Applicable Legislation; Evidence of Compliance - Applicable Legislation	
18.1.2	Intellectual property rights	Yes	Yes	Information Security Policies and Procedures - Intellectual property rights	
18.1.3	Protection of records	Yes	Yes	Information Security Policies and Procedures - Protection of records	
18.1.4	Privacy and protection of personally identifiable information	Yes	Yes	Information Security Policies and Procedures - Privacy and protection of personally identifiable information	
18.1.5	Regulation of cryptographic controls	Yes	Yes	Information Security Policies and Procedures - Regulation of cryptographic controls	
18.2	Independent review of information security				
18.2	Independent review of information security	Yes	Yes	Information Security Policies and Procedures - Information security review	
18.2.1	Compliance with security policies and standards	Yes	Yes	Information Security Policies and Procedures - Information security review	
18.2.2	Technical compliance review	Yes	Yes	Information Security Policies and Procedures - Information security review	