



# Microsoft Defender for Cloud

ISO 27001:2013 Compliance Report

5/1/2024 8:09:57 PM UTC

# Table of contents











- i. Executive summary
- ii. ISO 27001:2013 sections summary
- iii. ISO 27001:2013 controls status














## ISO 27001:2013 sections summary

The following is a summary status for each of the sections of the ISO 27001:2013. For each section, you will find the overall number of passing and failing controls, based on automated assessments run by Defender for Cloud.

A failing control indicates that at least one Defender for Cloud assessment associated with this control failed. A passing control indicates that all the Defender for Cloud assessments associated with this control passed. Note that status is shown only for supported controls, i.e. controls that have relevant Defender for Cloud assessments associated with them.

Area	Failed controls	Passed controls	
A.5. Information Security Policies	0	2	
A.6. Organization of Information Security	0	7	
A.7. Human Resources Security	0	6	
A.8. Asset Management	0	10	
A.9. Access Control	0	14	
A.10. Cryptography	0	2	
A.11. Physical And Environmental Security	0	15	
A.12. Operations Security	0	14	
A.13. Communications Security	0	7	
A.14. System Acquisition, Development And Maintenance	0	13	

A.15. Supplier Relationships	0	5	
A.16. Information Security Incident Management	0	7	
A.17. Information Security Aspects Of Business Continuity Management	0	4	
A.18. Compliance	0	8	
C.4. Context of the organization	0	4	
C.5. Leadership	0	16	
C.6. Planning	0	23	
C.7. Support	0	20	
C.8. Operation	0	3	
C.9. Performance Evaluation	0	23	
C.10. Improvement	0	4	



# ISO 27001:2013 controls status

The following is a summary status for each supported control of the ISO 27001:2013. For each control, you will find the overall number of passing, failing and skipped assessment associated with that control.


A failing assessment indicates a Defender for Cloud assessment that failed on at least one resource in your environment. A passing Defender for Cloud assessment indicates an assessment that passed on all resources. A skipped assessment indicates an assessment that was not run, whether because this assessment type is disabled or because there are no relevant resources in your environment.







Note that status is shown only for supported controls, i.e. controls that have relevant Defender for Cloud assessments associated with them.

## A.5. Information Security Policies







Control	Failed assessments	Passed assessments	Skipped assessments	
A.5.1.1. Policies for information security	0	0	41	
A.5.1.2. Review of the policies for information security	0	0	28	

## A.6. Organization of Information Security











Control	Failed assessments	Passed assessments	Skipped assessments	
A.6.1.1. Information security roles and responsibilities	0	0	72	

A.6.1.2. Segregation of Duties	0	2	3	
A.6.1.3. Contact with authorities	0	0	2	
A.6.1.4. Contact with special interest groups	0	0	6	
A.6.1.5. Information security in project management	0	0	25	
A.6.2.1. Mobile device policy	0	0	13	
A.6.2.2. Teleworking	0	0	16	


## A.7. Human Resources Security

Control	Failed assessments	Passed assessments	Skipped assessments	
A.7.1.1. Screening	0	0	3	
A.7.1.2. Terms and conditions of employment	0	0	24	
A.7.2.1. Management responsibilities	0	0	26	
A.7.2.2. Information security awareness, education and training	0	0	14	
A.7.2.3. Disciplinary process	0	0	2	
A.7.3.1. Termination or change of employment responsibilities	0	0	8	

## A.8. Asset Management

Control	Failed assessments	Passed assessments	Skipped assessments	
A.8.1.1. Inventory of assets	0	0	2	
A.8.1.2. Ownership of assets	0	0	7	
A.8.1.3. Acceptable use of assets	0	0	2	
A.8.1.4. Return of assets	0	0	8	
A.8.2.1. Classification of information	0	1	4	
A.8.2.2. Labelling of information	0	0	4	
A.8.2.3. Handling of assets	0	0	26	
A.8.3.1. Management of removable media	0	0	6	
A.8.3.2. Disposal of media	0	0	2	
A.8.3.3. Physical media transfer	0	0	2	


## A.9. Access Control

Control	Failed assessments	Passed assessments	Skipped assessments	
A.9.1.1. Access control policy	0	0	4	



A.9.1.2. Access to networks and network services	0	8	21	
A.9.2.1. User registration and de-registration	0	0	27	
A.9.2.2. User access provisioning	0	0	19	
A.9.2.3. Management of privileged access rights	0	7	26	
A.9.2.4. Management of secret authentication information of users	0	7	14	
A.9.2.5. Review of user access rights	0	4	13	
A.9.2.6. Removal or adjustment of access rights	0	2	15	
A.9.3.1. Use of secret authentication information	0	0	15	
A.9.4.1. Information access restriction	0	0	11	
A.9.4.2. Secure log-on procedures	0	3	14	
A.9.4.3. Password management system	0	8	14	
A.9.4.4. Use of privileged utility programs	0	0	9	
A.9.4.5. Access control to program source code	0	0	10	






## A.10. Cryptography

Control	Failed assessments	Passed assessments	Skipped assessments	
A.10.1.1. Policy on the use of cryptographic controls	0	11	7	








A.10.1.2. Key Management	0	0	15	
--------------------------	---	---	----	---

## A.11. Physical And Environmental Security

Control	Failed assessments	Passed assessments	Skipped assessments	
A.11.1.1. Physical security perimeter	0	0	8	
A.11.1.2. Physical entry controls	0	0	9	
A.11.1.3. Securing offices, rooms and facilities	0	0	5	
A.11.1.4. Protecting against external and environmental threats	0	0	9	
A.11.1.5. Working in secure areas	0	0	3	
A.11.1.6. Delivering and loading areas	0	0	5	
A.11.2.1. Equipment sitting and protection	0	0	1	
A.11.2.2. Supporting utilities	0	0	3	
A.11.2.3. Cabling security	0	0	4	
A.11.2.4. Equipment maintenance	0	0	9	

A.11.2.5. Removal of assets	0	0	6	
A.11.2.6. Security of equipment and assets off-premises	0	0	10	
A.11.2.7. Secure disposal or re-use of equipment	0	0	5	
A.11.2.8. Unattended user equipment	0	0	2	
A.11.2.9. Clear desk and clear screen policy	0	0	3	



## A.12. Operations Security

Control	Failed assessments	Passed assessments	Skipped assessments	
A.12.1.1. Documented operating procedures	0	0	30	
A.12.1.2. Change management	0	0	27	
A.12.1.3. Capacity management	0	0	2	
A.12.1.4. Separation of development, testing and operational environments	0	0	10	
A.12.2.1. Controls against malware	0	0	11	
A.12.3.1. Information backup	0	0	13	
A.12.4.1. Event Logging	0	5	48	










A.12.4.2. Protection of log information	0	0	8	
A.12.4.3. Administrator and operator logs	0	5	24	
A.12.4.4. Clock Synchronization	0	5	3	
A.12.5.1. Installation of software on operational systems	0	1	18	
A.12.6.1. Management of technical vulnerabilities	0	4	9	
A.12.6.2. Restrictions on software installation	0	1	18	
A.12.7.1. Information systems audit controls	0	0	1	





## A.13. Communications Security

Control	Failed assessments	Passed assessments	Skipped assessments	
A.13.1.1. Network controls	0	2	38	
A.13.1.2. Security of network services	0	0	16	
A.13.1.3. Segregation of networks	0	0	17	
A.13.2.1. Information transfer policies and procedures	0	2	30	
A.13.2.2. Agreements on information transfer	0	0	11	






A.13.2.3. Electronic messaging	0	0	10	
A.13.2.4. Confidentiality or non-disclosure agreements	0	0	14	

## A.14. System Acquisition, Development And Maintenance

Control	Failed assessments	Passed assessments	Skipped assessments	
A.14.1.1. Information security requirements analysis and specification	0	0	24	
A.14.1.2. Securing application services on public networks	0	0	32	
A.14.1.3. Protecting application services transactions	0	0	29	
A.14.2.1. Secure development policy	0	0	7	
A.14.2.2. System change control procedures	0	0	25	
A.14.2.3. Technical review of applications after operating platform changes	0	0	18	
A.14.2.4. Restrictions on changes to software packages	0	0	24	
A.14.2.5. Secure system engineering principles	0	0	5	
A.14.2.6. Secure development environment	0	0	10	





A.14.2.7. Outsourced development	0	0	28	
A.14.2.8. System security testing	0	0	8	
A.14.2.9. System acceptance testing	0	0	14	
A.14.3.1. Protection of test data	0	0	11	

## A.15. Supplier Relationships





Control	Failed assessments	Passed assessments	Skipped assessments	
A.15.1.1. Information security policy for supplier relationships	0	0	6	
A.15.1.2. Addressing security within supplier agreement	0	0	24	
A.15.1.3. Information and communication technology supply chain	0	0	4	
A.15.2.1. Monitoring and review of supplier services	0	0	4	
A.15.2.2. Managing changes to supplier services	0	0	15	

## A.16. Information Security Incident Management


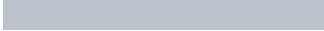
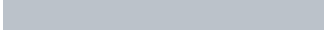

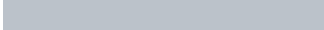

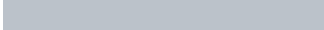

Control	Failed assessments	Passed assessments	Skipped assessments	
---------	--------------------	--------------------	---------------------	--

A.16.1.1. Responsibilities and procedures	0	0	7	
A.16.1.2. Reporting information security events	0	0	14	
A.16.1.3. Reporting information security weaknesses	0	0	4	
A.16.1.4. Assessment of and decision on information security events	0	0	23	
A.16.1.5. Response to information security incidents	0	0	12	
A.16.1.6. Learning from information security incidents	0	0	13	
A.16.1.7. Collection of evidence	0	0	7	


## A.17. Information Security Aspects Of Business Continuity Management

Control	Failed assessments	Passed assessments	Skipped assessments	
A.17.1.1. Planning information security continuity	0	0	11	
A.17.1.2. Implementing information security continuity	0	0	18	
A.17.1.3. Verify, review and evaluate information security continuity	0	0	3	
A.17.2.1. Availability of information processing facilities	0	0	17	




## A.18. Compliance

Control	Failed assessments	Passed assessments	Skipped assessments	
A.18.1.1. Identification applicable legislation and contractual requirements	0	0	29	
A.18.1.2. Intellectual property rights	0	0	2	
A.18.1.3. Protection of records	0	0	15	
A.18.1.4. Privacy and protection of personally identifiable information	0	0	6	
A.18.1.5. Regulation of cryptographic controls	0	0	2	
A.18.2.1. Independent review of information security	0	0	2	
A.18.2.2. Compliance with security policies and standards	0	0	35	
A.18.2.3. Technical compliance review	0	0	5	










## C.4. Context of the organization








Control	Failed assessments	Passed assessments	Skipped assessments	
C.4.3.a. Determining the scope of the information security management system	0	0	3	











C.4.3.b. Determining the scope of the information security management system	0	0	3	
C.4.3.c. Determining the scope of the information security management system	0	0	18	
C.4.4. Information security management system	0	0	5	
















## C.5. Leadership

Control	Failed assessments	Passed assessments	Skipped assessments	
C.5.1.a. Leadership and commitment	0	0	6	
C.5.1.b. Leadership and commitment	0	0	27	
C.5.1.c. Leadership and commitment	0	0	10	
C.5.1.d. Leadership and commitment	0	0	1	
C.5.1.e. Leadership and commitment	0	0	3	
C.5.1.f. Leadership and commitment	0	0	9	
C.5.1.g. Leadership and commitment	0	0	3	
C.5.1.h. Leadership and commitment	0	0	1	
C.5.2.a. Policy	0	0	4	

















C.5.2.b. Policy	0	0	4	
C.5.2.c. Policy	0	0	22	
C.5.2.d. Policy	0	0	22	
C.5.2.e. Policy	0	0	4	
C.5.2.f. Policy	0	0	4	
C.5.2.g. Policy	0	0	1	
C.5.3.b. Organizational roles, responsibilities and authorities	0	0	2	





## C.6. Planning

Control	Failed assessments	Passed assessments	Skipped assessments	
C.6.1.1.a. General	0	0	3	
C.6.1.1.b. General	0	0	3	
C.6.1.1.c. General	0	0	3	
C.6.1.1.d. General	0	0	3	
C.6.1.1.e.1. General	0	0	3	
C.6.1.1.e.2. General	0	0	3	
C.6.1.2.a.1. Information security risk assessment	0	0	2	
C.6.1.2.a.2. Information security risk assessment	0	0	2	




C.6.1.2.b. Information security risk assessment	0	0	1	
C.6.1.2.c.1. Information security risk assessment	0	0	2	
C.6.1.2.c.2. Information security risk assessment	0	0	2	
C.6.1.2.d.1. Information security risk assessment	0	0	2	
C.6.1.2.d.2. Information security risk assessment	0	0	2	
C.6.1.2.d.3. Information security risk assessment	0	0	2	
C.6.1.2.e.1. Information security risk assessment	0	0	2	
C.6.1.2.e.2. Information security risk assessment	0	0	2	
C.6.1.3.a. Information security risk treatment	0	0	1	
C.6.1.3.b. Information security risk treatment	0	0	1	
C.6.1.3.c. Information security risk treatment	0	0	1	
C.6.1.3.d. Information security risk treatment	0	0	1	
C.6.1.3.e. Information security risk treatment	0	0	1	
C.6.1.3.f. Information security risk treatment	0	0	1	
C.6.2.e. Information security objectives and planning to achieve them	0	0	2	

## C.7. Support



Control	Failed assessments	Passed assessments	Skipped assessments	
C.7.1. Resources	0	0	7	
C.7.2.a. Competence	0	0	3	
C.7.2.b. Competence	0	0	1	
C.7.2.c. Competence	0	0	1	
C.7.2.d. Competence	0	0	1	
C.7.3.a. Awareness	0	0	3	
C.7.3.b. Awareness	0	0	3	
C.7.3.c. Awareness	0	0	3	
C.7.4.a. Communication	0	0	4	
C.7.4.b. Communication	0	0	4	
C.7.4.c. Communication	0	0	4	
C.7.4.d. Communication	0	0	4	
C.7.4.e. Communication	0	0	4	
C.7.5.2.c. Creating and updating	0	0	1	
C.7.5.3.a. Control of documented information	0	0	1	
C.7.5.3.b. Control of documented information	0	0	3	

















C.7.5.3.c. Control of documented information	0	0	1	
C.7.5.3.d. Control of documented information	0	0	3	
C.7.5.3.e. Control of documented information	0	0	3	
C.7.5.3.f. Control of documented information	0	0	7	






## C.8. Operation

Control	Failed assessments	Passed assessments	Skipped assessments	
C.8.1. Operational planning and control	0	0	21	
C.8.2. Information security risk assessment	0	0	3	
C.8.3. Information security risk treatment	0	0	4	




## C.9. Performance Evaluation

Control	Failed assessments	Passed assessments	Skipped assessments	
C.9.1.a. Monitoring, measurement, analysis and evaluation	0	0	3	
C.9.1.b. Monitoring, measurement, analysis and evaluation	0	0	3	

C.9.1.c. Monitoring, measurement, analysis and evaluation	0	0	3	
C.9.1.d. Monitoring, measurement, analysis and evaluation	0	0	3	
C.9.1.e. Monitoring, measurement, analysis and evaluation	0	0	3	
C.9.1.f. Monitoring, measurement, analysis and evaluation	0	0	3	
C.9.2.a.1. Internal audit	0	0	1	
C.9.2.a.2. Internal audit	0	0	1	
C.9.2.b. Internal audit	0	0	1	
C.9.2.c. Internal audit	0	0	2	
C.9.2.d. Internal audit	0	0	1	
C.9.2.e. Internal audit	0	0	5	
C.9.2.f. Internal audit	0	0	1	
C.9.2.g. Internal audit	0	0	3	
C.9.3.a. Management review	0	0	5	
C.9.3.b. Management review	0	0	4	
C.9.3.c.1. Management review	0	0	6	
C.9.3.c.2. Management review	0	0	4	

C.9.3.c.3. Management review	0	0	4	
C.9.3.c.4. Management review	0	0	4	
C.9.3.d. Management review	0	0	3	
C.9.3.e. Management review	0	0	3	
C.9.3.f. Management review	0	0	3	

## C.10. Improvement

Control	Failed assessments	Passed assessments	Skipped assessments	
C.10.1.d. Nonconformity and corrective action	0	0	1	
C.10.1.e. Nonconformity and corrective action	0	0	1	
C.10.1.f. Nonconformity and corrective action	0	0	3	
C.10.1.g. Nonconformity and corrective action	0	0	3	