



# Microsoft Defender for Cloud

SOC 2 Compliance Report

11/27/2023 9:06:03 AM UTC

# Table of contents

- i. Executive summary
- ii. SOC 2 sections summary
- iii. SOC 2 controls status

# Executive summary

## Introduction

Microsoft Defender for Cloud executes a set of automated assessments on your Cloud environment which can help provide evidence relevant to specific controls in a compliance framework or standard. This report summarizes the current status of those assessments on your environment, as they map to the associated controls. This report does not represent a complete compliance report for the standard, nor does it ensure compliance.

## Compliance with SOC 2 controls

Your environment is compliant with 61 of 61 supported SOC 2 controls.



## Coverage

Subscriptions: 1











resources: 272



Subscription Name	Subscription ID
Statement-Matching.com	d3f3d452-1bdc-477c-8849-6d9659f8b53c

## SOC 2 sections summary

The following is a summary status for each of the sections of the SOC 2. 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	
A1. Additional Criteria For Availability	0	3	
CC1. Control Environment	0	5	
CC2. Communication and Information	0	3	
CC3. Risk Assessment	0	4	
CC4. Monitoring Activities	0	2	
CC5. Control Activities	0	3	
CC6. Logical and Physical Access Controls	0	8	
CC7. System Operations	0	5	
CC8. Change Management	0	1	
CC9. Risk Mitigation	0	2	

C1. Additional Criteria For Confidentiality	0	2	
P1. Additional Criteria For Privacy	0	1	
P2. Additional Criteria For Privacy	0	1	
P3. Additional Criteria For Privacy	0	2	
P4. Additional Criteria For Privacy	0	3	
P5. Additional Criteria For Privacy	0	2	
P6. Additional Criteria For Privacy	0	7	
P7. Additional Criteria For Privacy	0	1	
P8. Additional Criteria For Privacy	0	1	
P11. Additional Criteria For Processing Integrity	0	5	



# SOC 2 controls status

The following is a summary status for each supported control of the SOC 2. 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.

## A1. Additional Criteria For Availability




Control	Failed assessments	Passed assessments	Skipped assessments	
A1.1. Capacity management	0	0	1	
A1.2. Environmental protections, software, data back-up processes, and recovery infrastructure	0	4	9	
A1.3. Recovery plan testing	0	0	4	

## CC1. Control Environment





Control	Failed assessments	Passed assessments	Skipped assessments	
CC1.1. COSO Principle 1	0	0	8	

CC1.2. COSO Principle 2	0	0	5	
CC1.3. COSO Principle 3	0	0	5	
CC1.4. COSO Principle 4	0	0	5	
CC1.5. COSO Principle 5	0	0	4	

## CC2. Communication and Information

Control	Failed assessments	Passed assessments	Skipped assessments	
CC2.1. COSO Principle 13	0	0	3	
CC2.2. COSO Principle 14	0	3	6	
CC2.3. COSO Principle 15	0	3	11	

## CC3. Risk Assessment

Control	Failed assessments	Passed assessments	Skipped assessments	
CC3.1. COSO Principle 6	0	0	7	
CC3.2. COSO Principle 7	0	3	8	
CC3.3. COSO Principle 8	0	0	1	
CC3.4. COSO Principle 9	0	0	6	

## CC4. Monitoring Activities

Control	Failed assessments	Passed assessments	Skipped assessments	
CC4.1. COSO Principle 16	0	0	3	
CC4.2. COSO Principle 17	0	0	2	

## CC5. Control Activities

Control	Failed assessments	Passed assessments	Skipped assessments	
CC5.1. COSO Principle 10	0	0	2	
CC5.2. COSO Principle 11	0	4	14	
CC5.3. COSO Principle 12	0	0	4	

## CC6. Logical and Physical Access Controls

Control	Failed assessments	Passed assessments	Skipped assessments	
CC6.1. Logical access security software, infrastructure, and architectures	0	38	42	
CC6.2. Access provisioning and removal	0	3	8	
CC6.3. Rol based access and least privilege	0	9	11	
CC6.4. Restricted physical access	0	0	1	



CC6.5. Logical and physical protections over physical assets	0	0	2	
CC6.6. Security measures against threats outside system boundaries	0	24	17	
CC6.7. Restrict the movement of information to authorized users	0	17	13	
CC6.8. Prevent or detect against unauthorized or malicious software	0	42	11	

## CC7. System Operations

Control	Failed assessments	Passed assessments	Skipped assessments	
CC7.1. Detection and monitoring of new vulnerabilities	0	5	12	
CC7.2. Monitor system components for anomalous behavior	0	12	6	
CC7.3. Security incidents detection	0	0	1	
CC7.4. Security incidents response	0	4	13	
CC7.5. Recovery from identified security incidents	0	4	15	

## CC8. Change Management

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

CC8.1. Changes to infrastructure, data, and software	0	36	16	
--	---	----	----	--

## CC9. Risk Mitigation

Control	Failed assessments	Passed assessments	Skipped assessments	
CC9.1. Risk mitigation activities	0	0	3	
CC9.2. Vendors and business partners risk management	0	0	20	


## C1. Additional Criteria For Confidentiality

Control	Failed assessments	Passed assessments	Skipped assessments	
C1.1. Protection of confidential information	0	0	3	
C1.2. Disposal of confidential information	0	0	3	



## P1. Additional Criteria For Privacy

Control	Failed assessments	Passed assessments	Skipped assessments	
P1.1. Privacy notice	0	0	5	




## P2. Additional Criteria For Privacy

Control	Failed assessments	Passed assessments	Skipped assessments	
P2.1. Privacy consent	0	0	4	


### P3. Additional Criteria For Privacy

Control	Failed assessments	Passed assessments	Skipped assessments	
P3.1. Consistent personal information collection	0	0	4	
P3.2. Personal information explicit consent	0	0	2	

### P4. Additional Criteria For Privacy








Control	Failed assessments	Passed assessments	Skipped assessments	
P4.1. Personal information use	0	0	5	
P4.2. Personal information retention	0	0	2	
P4.3. Personal information disposal	0	0	2	

### P5. Additional Criteria For Privacy


Control	Failed assessments	Passed assessments	Skipped assessments	
P5.1. Personal information access	0	0	2	

P5.2. Personal information correction	0	0	1	
---------------------------------------	---	---	---	---


## P6. Additional Criteria For Privacy

Control	Failed assessments	Passed assessments	Skipped assessments	
P6.1. Personal information third party disclosure	0	0	15	
P6.2. Authorized disclosure of personal information record	0	0	1	
P6.3. Unauthorized disclosure of personal information record	0	0	1	
P6.4. Third party agreements	0	0	1	
P6.5. Third party unauthorized disclosure notification	0	0	12	
P6.6. Privacy incident notification	0	0	2	
P6.7. Accounting of disclosure of personal information	0	0	5	





## P7. Additional Criteria For Privacy

Control	Failed assessments	Passed assessments	Skipped assessments	
P7.1. Personal information quality	0	0	3	

## P8. Additional Criteria For Privacy

Control	Failed assessments	Passed assessments	Skipped assessments	
P8.1. Privacy complaint management and compliance management	0	0	5	

## PI1. Additional Criteria For Processing Integrity

Control	Failed assessments	Passed assessments	Skipped assessments	
PI1.1. Data processing definitions	0	0	3	
PI1.2. System inputs over completeness and accuracy	0	0	1	
PI1.3. System processing	0	0	5	
PI1.4. System output is complete, accurate, and timely	0	0	3	
PI1.5. Store inputs and outputs completely, accurately, and timely	0	4	6	