



Azure Security Center

SOC TSP Compliance Report

12/26/2020 5:04:05 PM UTC

Table of contents

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

Executive summary

Introduction

Azure Security Center executes a set of automated assessments on your Azure 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 TSP controls

Your environment is compliant with 2 of 13 supported SOC TSP controls.



Coverage

subscriptions: 1






resources: 31

Subscription Name	Subscription ID
Azure Pass - Sponsorship	60944aff-0f61-4795-8f69-e06bb5fc0928

SOC TSP sections summary

The following is a summary status for each of the sections of the SOC TSP. For each section, you will find the overall number of passing and failing controls, based on automated assessments run by Security Center.

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

Area	Failed controls	Passed controls	
CC5. Common Criteria Related to Logical and Physical Access Controls	7	0	
CC6. Common Criteria Related to System Operations	2	0	
CC7. Common Criteria Related to Change Management	0	1	
A1. Additional Criteria for Availability	0	1	
C1. Additional Criteria for Confidentiality	2	0	


SOC TSP controls status





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



A failing assessment indicates a Security Center assessment that failed on at least one resource in your environment. A passing Security Center 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 Security Center assessments associated with them.


CC5. Common Criteria Related to Logical and Physical Access Controls


Control	Failed assessments	Passed assessments	Skipped assessments	
CC5.1. Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	11	55	0	

CC5.2. New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	7	47	0	
CC5.3. Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	7	45	0	
CC5.4. Access to data, software, functions, and other IT resources is authorized and modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	7	48	0	
CC5.6. Logical access security measures have been implemented to protect against security, availability, processing integrity, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	19	136	0	


CC5.7. The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	3	21	0	
CC5.8. Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.	11	94	0	

CC6. Common Criteria Related to System Operations


Control	Failed assessments	Passed assessments	Skipped assessments	
CC6.1. Vulnerabilities of system components to security, availability, processing integrity, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	5	65	0	

CC6.2. Security, availability, processing integrity, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	3	36	0	
---	---	----	---	---

CC7. Common Criteria Related to Change Management

Control	Failed assessments	Passed assessments	Skipped assessments	
CC7.2. Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security, availability, processing integrity, and confidentiality.	0	8	0	

A1. Additional Criteria for Availability

Control	Failed assessments	Passed assessments	Skipped assessments	
A1.2. Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	0	3	0	

C1. Additional Criteria for Confidentiality

Control	Failed assessments	Passed assessments	Skipped assessments	
C1.2. Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition in accordance with confidentiality commitments and requirements.	22	177	0	<div><div></div></div>
C1.3. Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties in accordance with confidentiality commitments and requirements.	7	44	0	<div><div></div></div>