Azure Security Center

ISO 27001 Compliance Report

5/6/2021 9:51:55 PM UTC

Table of contents

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 ISO 27001 controls

Your environment is compliant with 20 of 20 supported ISO 27001 controls.

ISO 27001 sections summary

The following is a summary status for each of the sections of the ISO 27001. 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	
A6. Organization of information security	0	1	
A9. Access control	0	7	
A10. Cryptography	0	1	
A12. Operations security	0	8	
A13. Communications security	0	3	

ISO 27001 controls status

The following is a summary status for each supported control of the ISO 27001. 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.

A6. Organization of information security

Control	Failed assessments	Passed assessments	Skipped assessments	
A6.1.2. Segregation of duties	0	2	0	

A9. Access control

Control	Failed assessments	Passed assessments	Skipped assessments	
A9.1.2. Access to networks and network services	0	46	0	
A9.2.3. Management of privileged access rights	0	49	0	
A9.2.4. Management of secret authentication information of users	0	3	0	

A9.2.5. Review of user access rights	0	4	0	
A9.2.6. Removal or adjustment of access rights	0	2	0	
A9.4.1. Information access restriction	0	43	0	
A9.4.2. Secure log-on procedures	0	12	0	

A10. Cryptography

Control	Failed assessments	Passed assessments	Skipped assessments	
A10.1.1. Policy on the use of cryptographic controls	0	9	0	

A12. Operations security

Control	Failed assessments	Passed assessments	Skipped assessments	
A12.2.1. Controls against malware	0	2	0	
A12.3.1. Information backup	0	3	0	
A12.4.1. Event logging	0	79	0	
A12.4.3. Administrator and operator logs	0	43	0	
A12.4.4. Clock synchronization	0	11	0	

A12.5.1. Installation of software on operational systems	0	1	0	
A12.6.1. Management of technical vulnerabilities	0	7	0	
A12.6.2. Restrictions on software installation	0	1	0	

A13. Communications security

Control	Failed assessments	Passed assessments	Skipped assessments	
A13.1.1. Network controls	0	6	0	
A13.1.2. Security of network services	0	8	1	
A13.2.1. Information transfer policies and procedures	0	5	0	