



Azure Security Center

NIST SP 800 53 R4 Compliance Report

12/26/2020 5:04:25 PM UTC

Table of contents

- i. Executive summary
- ii. NIST SP 800 53 R4 sections summary
- iii. NIST SP 800 53 R4 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 NIST SP 800 53 R4 controls

Your environment is compliant with 10 of 29 supported NIST SP 800 53 R4 controls.



Coverage

subscriptions: 1









resources: 31

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

NIST SP 800 53 R4 sections summary

The following is a summary status for each of the sections of the NIST SP 800 53 R4. 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	
AC. Access Control	4	4	
AU. Audit and Accountability	4	0	
CM. Configuration Management	0	3	
CP. Contingency Planning	1	0	
IA. Identification and Authentication	1	1	
RA. Risk Assessment	0	1	
SC. System and Communications Protection	5	1	
SI. System and Information Integrity	4	0	







NIST SP 800 53 R4 controls status

The following is a summary status for each supported control of the NIST SP 800 53 R4. 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.

AC. Access Control

Control	Failed assessments	Passed assessments	Skipped assessments	
AC.2.*. Additional assessments for AC.2 - Account Management	0	5	0	
AC.2.7. Role-Based Schemes	1	1	0	
AC.2.12. Account Monitoring / Atypical Usage	1	0	0	
AC.4.*. Additional assessments for AC.4 - Information Flow Enforcement	0	3	0	
AC.5. Separation of Duties	1	1	0	
AC.6.7. Review of User Privileges	1	1	0	

AC.16.*. Additional assessments for AC.16 - Security Attributes	0	2	0	<div></div>
AC.17.1. Automated Monitoring / Control	0	3	0	<div></div>

AU. Audit and Accountability

Control	Failed assessments	Passed assessments	Skipped assessments	
AU.3.2. Centralized Management of Planned Audit Record Content	1	2	0	<div></div>
AU.5.*. Additional assessments for AU.5 - Response to Audit Processing Failures	2	2	0	<div></div>
AU.6.4. Central Review and Analysis	1	2	0	<div></div>
AU.12.*. Additional assessments for AU.12 - Audit Generation	3	4	0	<div></div>

CM. Configuration Management

Control	Failed assessments	Passed assessments	Skipped assessments	
CM.7.2. Prevent Program Execution	0	0	1	<div></div>
CM.7.5. Authorized Software / Whitelisting	0	0	1	<div></div>
CM.11.*. Additional assessments for CM.11 - User-Installed Software	0	0	1	<div></div>

CP. Contingency Planning

Control	Failed assessments	Passed assessments	Skipped assessments	
CP.7.*. Additional assessments for CP.7 - Alternate Processing Site	1	0	0	<div><div></div></div>

IA. Identification and Authentication

Control	Failed assessments	Passed assessments	Skipped assessments	
IA.2.1. Network Access to Privileged Accounts	1	1	0	<div><div></div><div></div></div>
IA.2.2. Network Access to Non-Privileged Accounts	0	1	0	<div><div></div></div>

RA. Risk Assessment

Control	Failed assessments	Passed assessments	Skipped assessments	
RA.5.*. Additional assessments for RA.5 - Vulnerability Scanning	0	3	1	<div><div></div><div></div></div>

SC. System and Communications Protection

Control	Failed assessments	Passed assessments	Skipped assessments	
SC.5.*. Additional assessments for SC.5 - Denial of Service Protection	0	0	1	<div><div></div></div>

SC.7.*. Additional assessments for SC.7 - Boundary Protection	1	1	0	<div><div></div><div></div></div>
SC.7.3. Access Points	1	0	0	<div><div></div></div>
SC.7.4. External Telecommunications Services	1	0	0	<div><div></div></div>
SC.8.1. Cryptographic or Alternate Physical Protection	1	5	0	<div><div></div><div></div></div>
SC.28.1. Cryptographic Protection	2	3	0	<div><div></div><div></div></div>

SI. System and Information Integrity

Control	Failed assessments	Passed assessments	Skipped assessments	
SI.2.*. Additional assessments for SI.2 - Flaw Remediation	1	2	1	<div><div></div><div></div><div></div></div>
SI.3.*. Additional assessments for SI.3 - Malicious Code Protection	1	2	1	<div><div></div><div></div><div></div></div>
SI.3.1. Central Management	1	2	1	<div><div></div><div></div><div></div></div>
SI.4.*. Additional assessments for SI.4 - Information System Monitoring	1	4	0	<div><div></div><div></div></div>