

Armor Anywhere Compliance Matrix
Compliance Made Easy

rackspace[®]



Armor Anywhere Compliance Matrix

The Armor Compliance Matrix is intended to help IT, IT Security, and Compliance teams understand how Armor accelerates adherence to major compliance mandates their organizations are subject to.

Armor Security Services	PCI DSS 3.2.1 Controls	HIPAA/HITECH Controls	HITRUST CSF v9.3 (66 Controls Required for Certification)	GDPR	DFS 500 (23 NYCRR 500)	Risk Mitigation
Network layer						
Intrusion Detection	11.4	Security best practice - implied control under 164.306(A)	09.m(HT2)	Article 32, Section 1(b)	500.02 (a), (b)(2), (b)(3)	Malicious allowed traffic
Internal Network Vulnerability Scanning ⁽¹⁾	11.2.3	Included in §164.308(a)(1)	10.m	Article 32, Section 1(d)	500.02 (a), (b)(2), (b)(3) 500.05 (b)	Exploits due to missing patches/updates; improper network firewall configuration
Server layer						
File Integrity Monitoring ⁽²⁾	11.5	§164.312(e)	09.ab, 10.h	Article 32, Section 1(b) 5	500.02 (a), (b)(2), (b)(3)	Monitoring unauthorized changes to critical files
Malware Protection	5.1, 5.2, 5.3	§164.308(a)(5)(ii)(B)	09.ab, 10.h	Article 32, Section 1(b)	500.02 (a), (b)(2), (b)(3)	Compromise due to virus/malware infection
Log Management ⁽⁴⁾	10.1, 10.2.2-10.2.7, 10.3, 10.5, 10.6, 10.7	§164.308(a)(1)(ii)(D), §164.308(a)(5)(ii)(C), §164.312(b)	09.aa, 09.ab, 09.ac	Article 32, Section 1(b) and 1(d)	500.02 (3), (4) 500.06 (a) (2) - see special note	Detection of malicious activity (security incidents)
Patching Monitoring ⁽³⁾	6.1, 6.2	Security best practice - implied control under 164.306(A)	10.m	Article 32, Section 1(b)	500.02 (a)	OS and COTS software weaknesses
Administrative controls						
Incident Response ⁽⁵⁾	12.10	§164.308(a)(6)	05.b, 11.a, 11.c	Article 32, Section 1(b)	500.16 - see special note 500.10 (a), (b) 500.17	Response to security incidents
Multi-factor Authentication for AMP access ⁽⁶⁾	N/A	N/A	N/A	N/A	500.12 (b)	Unauthorized remote use of administrative access
Business Associate Contract	N/A	§164.308(b)(1)	05.k(HT2), 09.e(HT2)	N/A	N/A	Legal liability for data loss/breach
Access Control ⁽⁷⁾	7.1.1, 7.1.2	§164.312(a)(1)(12)	01.a	Article 32, Section 1(b)	500.07	Unauthorized access
Security Audits ⁽⁸⁾	Security best practice	§164.308(a)(8)	06.g	Article 32, Section 1(d)	500.02 (b)(1) 500.11 - see special note	Validation of security controls program

1. The service collects basic asset identification information, Windows registry information (for Windows systems only) and file version and package information periodically throughout each day and reports the results to the scan platform that assesses the data and determines the vulnerabilities that exist. Armor posts vulnerability information in AMP weekly that represents the state of the instance as of the last report.

Note: Armor does not provide any patches or updates.

- This control is only applicable to OS files for the servers protected by Armor Anywhere. Customization to cover customer specific files is available at an additional cost.
- Armor provides a report highlighting any missing critical/security patches against the vendor-supplied OS and other COTS software installed on the server. Customer is responsible for the installation of all patches for both the OS and all applications they install.
- Armor provides automated log reviews and reports exceptions to the customer for further review. The reviews are limited to operating system logs for customer virtual servers, and the malware protection, file integrity monitoring and intrusion detection services. Collection and review of customer application and other logs are the responsibility of the customer. Application logs as well as the device and cloud specific logs can be collected and analyzed at an additional cost. Default retention for all logs is 30 days with an option for 13 month retention available at an additional cost.

Special note for DFS 500: Customers are required to retain logs for 3 years and will therefore need to export their logs from AMP to meet this requirement.

- Special note for DFS 500: Armor's Security Operations Centre SOC fulfills these requirements for the services provided and for our IR service.
- Coverage for this control is limited to access to the Armor Management Portal (AMP)
- Relates to the provisioning and use of the Armor administrative account included with each secure server.
- Applies to Armor's third party attestations that include PCI DSS validation, HITRUST certification, ISO 27001:2013 certification and SOC 2 Type II reports.

Special note for DFS 500: Armor's third party audit attestations assist CEs with their 3rd party vendor management requirements. HT1. There are 66 controls required to meet the HITRUST CSF.

About Rackspace

At Rackspace, we accelerate the value of the cloud during every phase of digital transformation. By managing apps, data, security and multiple clouds, we are the best choice to help customers get to the cloud, innovate with new technologies and maximize their IT investments. As a recognized Gartner Magic Quadrant leader, we are uniquely positioned to close the gap between the complex reality of today and the promise of tomorrow. Passionate about customer success, we provide unbiased expertise, based on proven results, across all the leading technologies. And across every interaction worldwide, we deliver Fanatical Experience™. Rackspace has been honored by Fortune, Forbes, Glassdoor and others as one of the best places to work.

Learn more at www.rackspace.com or call at 1-800-961-2888.

© 2020 Rackspace US, Inc. :: Rackspace®, Fanatical Experience™ and other Rackspace marks are either service marks or registered service marks of Rackspace US, Inc. in the United States and other countries. All other trademarks, service marks, images, products and brands remain the sole property of their respective holders and do not imply endorsement or sponsorship.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS A GENERAL INTRODUCTION TO RACKSPACE® SERVICES AND DOES NOT INCLUDE ANY LEGAL COMMITMENT ON THE PART OF RACKSPACE.

You should not rely solely on this document to decide whether to purchase the service. Rackspace detailed services descriptions and legal commitments are stated in its services agreements. Rackspace services' features and benefits depend on system configuration and may require enabled hardware, software or additional service activation.

Except as set forth in Rackspace general terms and conditions, cloud terms of service and/or other agreement you sign with Rackspace, Rackspace assumes no liability whatsoever, and disclaims any express or implied warranty, relating to its services including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, and noninfringement.

Although part of the document explains how Rackspace services may work with third party products, the information contained in the document is not designed to work with all scenarios. any use or changes to third party products and/or configurations should be made at the discretion of your administrators and subject to the applicable terms and conditions of such third party. Rackspace does not provide technical support for third party products, other than specified in your hosting services or other agreement you have with Rackspace and Rackspace accepts no responsibility for third-party products.

Rackspace cannot guarantee the accuracy of any information presented after the date of publication.

February 19, 2020 / Rackspace-Armor-Anywhere-Detailed-Compliance-Matrix-SAL-TSK-667