Rackspace Security Essentials
Compliance Matrix

# Compliance Made Easy

# Security Essentials Compliance Matrix

This matrix is intended to help IT, IT Security, and Compliance teams understand how Rackspace Technology and Armor can help accelerate adherence to major compliance mandates their organizations are subject to. These compliance controls are available for the Rackspace Security Essentials services and the Rackspace Proactive Detection and Response service.

| | 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.

2. This control is only applicable to OS files for the servers protected by Security Essentials or the Proactive Detection and Response service. Customization to cover customer specific files is available at an additional cost.

3. 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.

4. 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 Security Operations Center (SOC) fulfills these requirements for the services provided and for our IR service.

5. Coverage for this control is limited to access to the Armor Management Portal (AMP).

6. Relates to the provisioning and use of the Armor administrative account included with each secure server.

7. Applies to the 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 third party vendor management requirements. There are 66 controls required to meet the HITRUST CSF.

# About Rackspace Technology

Rackspace Technology is the multicloud solutions expert. We combine our expertise with the world's leading technologies — across applications, data and security — to deliver end-to-end solutions. We have a proven record of advising customers based on their business challenges, designing solutions that scale, building and managing those solutions, and optimizing returns into the future.

As a global, multicloud technology services pioneer, we deliver innovative capabilities of the cloud to help customers build new revenue streams, increase efficiency and create incredible experiences. Named a best place to work, year after year according to Fortune, Forbes, and Glassdoor, we attract and develop world-class talent to deliver the best expertise to our customers. Everything we do is wrapped in our obsession with our customers' success — our Fanatical Experience™ — so they can work faster, smarter and stay ahead of what's next.

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



May 12, 2021 / Rackspace-Other-Armor-Anywhere-Detailed-Compliance-Matrix-SAL-TSK-4614