

CHEAT SHEET:

PCI DSS 3.2 COMPLIANCE

WHAT IS PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements and industry best practices for preventing unauthorized access to cardholder data, including debit, credit, pre-paid, e-purse, ATM, and point-of-sale (POS) card brands.

PCI DSS REQUIREMENTS:

CONTROL OBJECTIVES	PCI DSS REQUIREMENTS
BUILD AND MAINTAIN A SECURE NETWORK	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
PROTECT CARDHOLDER DATA	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	<ol style="list-style-type: none">5. Protect all systems against malware and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
IMPLEMENT STRONG ACCESS CONTROL MEASURES	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need-to-know8. Identify and authenticate access to system components9. Restrict physical access to cardholder data
REGULARLY MONITOR AND TEST NETWORKS	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
MAINTAIN AN INFORMATION SECURITY POLICY	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for all personnel

WHO NEEDS TO BE PCI DSS COMPLIANT?

- Any entity that stores, processes or transmits cardholder data
- There are four merchant levels and their compliance requirements vary depending on their combined transaction volumes

	FILE ANNUAL REPORT OF COMPLIANCE (ROC), VALIDATED BY A QUALIFIED SECURITY ASSESSOR (QSA)	COMPLETE AN ANNUAL SELF-ASSESSMENT QUESTIONNAIRE (SAQ)	CONDUCT A QUARTERLY NETWORK SCAN BY AN APPROVED SCANNING VENDOR (ASV)	SUBMIT AN ATTESTATION OF COMPLIANCE (AOC) FORM
LEVEL 1 Over 6 million Visa and/or Mastercard transactions processed per year	✓		✓	✓
LEVEL 2 1 million to 6 million Visa and/or Mastercard transactions processed per year		✓	✓	✓
LEVEL 3 20,000 to 1 million Visa and/or Mastercard e-commerce transactions processed per year		✓	✓	✓
LEVEL 4 Merchants processing less than 20,000 Visa ecommerce transactions annually and all other merchants processing up to 1 million Visa transactions annually		✓	✓	✓

WHAT HAPPENS IF AN ORGANIZATION DOESN'T COMPLY?

- Increased risk of payment card data compromise
- Subject to fines
- Loss of credit card acceptance privileges

ALERT LOGIC SERVICE OFFERINGS FOR PCI DSS 3.2 COMPLIANCE

The integrated services that make up Alert Logic® address a broad range of PCI DSS 3.2 requirements to help you prevent unauthorized access to customer cardholder data.

SERVICE OFFERINGS	REQUIREMENT	
ALERT LOGIC MDR ESSENTIALS Asset Discovery, Vulnerability Analysis, and Endpoint Detection	6.1	Identify newly discovered security vulnerabilities
	11.2	Perform network vulnerability scans by an ASV at least quarterly or after any significant network change (Includes 11.2.1, 11.2.2 and 11.2.3)
ALERT LOGIC MDR PROFESSIONAL 24/7 Threat Management, Intrusion Detection, and Cloud Change Monitoring (Includes Essentials Capabilities)	10.1	Implement audit trails to link all access to system components to each individual user
	10.2	Automated audit trails
	10.3	Capture audit trails
	10.5	Secure logs
	10.5.5	Change detection to ensure integrity for log files
	10.6	Review logs at least daily
	10.7	Maintain logs online for three months
	10.7	Retain audit trail for at least one year
	11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the networks
11.5	Change detection to ensure integrity for critical system files, configuration files, or content files	
ALERT LOGIC MDR ENTERPRISE Threat Hunting & Custom Response (Includes Essentials & Professional Capabilities)	6.5	Have processes in place to protect applications from common vulnerabilities, such as injection flaws, buffer overflows and others
	6.6	Address new threats and vulnerabilities on an on-going basis and ensure these applications are protected against known attacks
	12.1	Implement an incident response plan. Be prepared to respond immediately to a system breach

PCI DSS FREQUENTLY ASKED QUESTIONS

QUESTION	ANSWER
Is Alert Logic a PCI DSS Approved Scanning Vendor (ASV)?	Yes. Alert Logic maintains ASV status.
Does Alert Logic have an Attestation of Compliance as a PCI DSS Service Provider?	Yes. Alert Logic maintains Level-2 SAQ Attestation of Compliance status.
What kind of responsibilities do customers have to make Alert Logic products and services address PCI DSS requirements?	Alert Logic customers must ensure that the products are monitoring the correct sources, and when Alert Logic notifies customers of issues in their environment, the customer must address the issues quickly. Also, customers are responsible for ensuring that the logs and other information sent to Alert Logic does not contain credit card data or any associated personal information. Details of these requirements are communicated in the contracts and during the Alert Logic onboarding and provisioning processes.
Does Alert Logic store logs long enough for PCI DSS requirements?	Yes. Alert Logic stores logs and provides customers access to them for one year. Customers also have the option of extending that time period.
I've seen several documents referring to Alert Logic as a PCI DSS Service Provider. What does that term mean?	The PCI Security Standards official glossary defines "Service Provider" as: "Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS, and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although it may be considered a service provider for other services)."
If I'm being audited, how can Alert Logic make the process easier?	Alert Logic provides access to configuration settings, security outcomes, documentation, and reports via web console that customers can show or provide to their QSA.



Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV) and maintains strict compliance with internal and external regulatory requirements for our IT operations and services, including: PCI DSS 3.2 Level 2 Audit, AICPA SOC 1 & 2 Audit, and ISO 27001-2013 certification for UK Operations.