

WHAT IS PCI-DSS?

The Payment Card Industry is a private industry group set up by the major credit card companies to define standards for companies that process credit card transactions. The Data Security Standard was defined to prevent credit card fraud, hacking and other security issues.

A company processing, storing, or transmitting credit card numbers must be PCI-DSS compliant or they risk losing the ability to process credit card payments. The PCI-DSS includes requirements covering network security, data protection, vulnerability management, access control, monitoring and testing, and information security.

According to the PCI Data Security Standard, an organisation must be able to monitor, report, and alert on attempted or successful access to systems and data security for those applications that contain sensitive cardholder data. **PCI-DSS explicitly calls for the collection and monitoring of event logs.**

LT Auditor+

Solutions for Payment Card Industry Data Security Standard (PCI-DSS)

HOW DOES LT AUDITOR+ HELP YOU MEET PCI-DSS REQUIREMENTS?

LT Auditor+ 9 for Windows provides the auditing mechanism for adhering to the following requirements set forth by the Payment Card Industry.

REQUIREMENT	LT AUDITOR+ PROVIDES
Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.	Audit, alerting & reporting functionality to effectively monitor & verify Active Directory changes.
Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Continuous monitoring of sensitive files and folders as well as Windows configuration settings within Active Directory & Group Policy.
Control addition, deletion, & modification of user IDs, credentials, & other identifier properties.	Active Directory auditing, alerting & reporting of user creations, deletions & modifications.
Immediately revoke access for any terminated users.	Auditing for verification of disabled or deleted accounts.

Cont'd...

...Cont'd

REQUIREMENT	LT AUDITOR+ PROVIDES
Remove/disable inactive user accounts at least every 90 days.	Auditing for verification of disabled or deleted accounts.
Do not use group, shared, or generic accounts & passwords.	The ability to filter & alert for use of group, shared or generic accounts to maintain compliance.
Limit repeated access attempts by locking out the user ID after not more than six attempts.	Auditing of locked accounts, with the ability to send real-time alerts when an account is locked, & scheduled reports delivered to any number of recipients.
Establish a process for linking all access to system components (especially those done with administrative privileges such as Administrator) to an individual user.	Comprehensive auditing, alerting & reporting capability on administrative activity within Active Directory, Group Policy, & the file system. The built-in Audit the Auditor service even audits changes to LT Auditor+'s configuration.
Implement automated audit trails to reconstruct events for all system components.	Full audit trails for audited servers & workstations, including USB storage device activity.
Track & monitor all user activities including user logons, user logoffs, user login failures, user added/deleted/modified, user logon failure/success on VPN servers, & success/failure of critical file access by users.	Auditing, alerting & reporting for all user activity including successful & failed logins, & logoffs, user creations, modifications or deletions & all file access attempts of audited files.
Record audit trail entries for each event for all system components.	Complete audit trails for changes to Windows Active Directory & Group Policy. LT Auditor+ audits, alerts & reports: <ul style="list-style-type: none"> • User identification (Who) • Type of event (What) • Date & time (When) • Success or failure (Enabled by filter) • Origination of event (Where) • Identity or name of affected data, system component, or resource (What)
Limit viewing of audit trails to those with a job related need.	Authenticated access to the Manager & Reporting Consoles. Additionally, any changes to permissions for viewing are recorded.
Protect audit trail files from unauthorised modifications.	Centralised audit data stored within its own MS-SQL Server or Oracle database. Database triggers can be configured to notify security of any unauthorised modification within the database.
Promptly back-up audit trail files to a centralised log server or media that is difficult to alter.	Facilities for archiving native Windows logs to any secure centralised location. LT Auditor+ data may be configured to archive on regular intervals.
Review logs for all system components at least daily.	A reporting console to create & schedule customised reports & automatically send the summary or detailed report at scheduled intervals.
Retain your audit trail history for a minimum of one year, with 3 months immediately available for analysis.	The ability to retain data for any number of years, constrained only by disk space availability on the hardware.

EVALUATION PROCESS

Evaluation available – download from www.altman.co.uk/auditing. For more information please contact our solutions team on 0113 273 0300 or email solutions@altman.co.uk.