**How to Comply to Requirement 10 of PCI DSS**

The requirement 10 of PCI Data Security Standard is one of the most important requirements since it is directly concerned with network access and security. Compliance to this requirement is majorly a task for the IT department and it curtails all those activities that are directly or indirectly involved in storing, processing and transmitting cardholder data through the network.

**Requirement 10: Track and monitor all access to network resources and cardholder data.**

According to this requirement, the organization should develop a system to keep a track of all activities on the network so that in case of breach of information the activity logs can trace the cause of the security breach. A good system should be able to generate report of every log and have a means to interpret those reports in an easy manner.

**10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.**

System components form an integral part of the network and hence any change in the system components has a direct effect on the network. For complying to this requirement it is important to keep a track of every time there is an access to the system components so that in case of any unwanted change in the network, it is easy to check which user was responsible for the change. Every user, particularly the administrators, should be monitored over the network and their activities should be checked. Regular report should be generated that gives a list of users accessing specific system objects. A report on every user on the network should also be generated that describes what each user is doing over the network.

**10.2 Implement automated assessment trails for all system components to reconstruct the following events.**

Although it may seem favorable to keep a track of system component access, it is not that easy when it is done manually. It is therefore recommended to automate the access tracking procedure, or to recreate the events.

The sub-sections of this requirement help us find out how compliance can be achieved through this requirement.

**10.2.1 All individual user accesses to cardholder data.**

The process to track and monitor user access to cardholder data should be automated to avoid any human error. Besides this, every user activity during log-in time should also be recorded. The data should further be sorted out in such a manner that the users who made access to important and private information over the network should be separated from the rest. This would help to achieve compliance to PCI DSS.

**10.2.2 All actions taken by any individual with root or administrative privileges.**

Administrators have full control over a network and they can easily have access to all sensitive information related to cardholder data. It is therefore important for compliance to this requirement that any access to cardholder data by the users with administrative rights should be constantly tracked. This tracking should be done by keeping a record of the administrator user name, the areas accessed by the particular user, the changes made by them, and the time spent by them.

**10.2.3 Access to all audit trails.**

For compliance to this requirement, companies need to verify any access to audit logs as they are often altered by individuals with fraudulent intentions. Keeping a check on audit log access will allow discovering if any changes, addition or deletion has been made by a particular user name.

**10.2.4 Invalid Logical Access attempts.**

Every user has to log in to the network when they have to access a resource. A login that is successful means that the user knew the actual username and password and entered into the system without any effort. But a failed login can be suspicious and means that someone outside the system is trying to access the network. It is important to keep a track of all such invalid login attempts. For compliance, it is necessary to monitor the trend of such activities, i.e. if they occur mostly at any specific time or if a particular username is more prone to such attempts, etc. The process should be automated so that any possibility of human error is ruled out. All login activities should be enlisted and unsuccessful or invalid attempts should be separated out to further perform their trend analysis.

**10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.**

If it is not known which users were logged in at the time of an incident, it is not possible to identify users that may have been involved. Hence it should be verified that every authentication and identification mechanism is logged.

**10.2.6 Initialization of Assessment Logs.**

Assessment logs are important to keep a check on every activity taking place on a network, especially the administrative activities. If the log data is cleared, it will also clear any evidence related to access logs. Hence, it is important that in order to comply to the above requirement, all audit log clearing actions should be recorded and any individual found guilty of log clearing should be questioned. To limit the possibility of such an event, it is important to restrict the rights of log clearing to a few authorized individuals only.

**10.2.7 Creation and Deletion of System Level Objects.**

System Level Objects control the system and network functionality. Every access to the system level objects needs to be closely monitored, but what is more important is the monitoring of any creation and deletion of these objects. To achieve this, it is important to log every user activity on system level objects, such as the name of the user, his access rights, and the time of access. This data can further help finding out whether there was any creation and/or deletion at that particular time when the user accessed the particular area. To achieve full compliance to this requirement, it is recommended to isolate all system level objects and get the record of all activities on those objects.

**10.3 Record at least the following audit trail entries for all system components for each event:**

* **User Identification**
* **Type of Event**
* **Date and Time**
* **Success or Failure Indication**
* **Origination of Event**
* **Identity or name of effected data, system component, or resource**

Recording these trail entries for all events mentioned in requirement 10.2, any breach of data can be quickly and easily identified, along with the details of who, when, where, what and how.

**10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.**

Time synchronization technology helps in synchronizing clocks on a number of systems. If these clocks are not synchronized properly, it gets difficult to compare different log files in different systems to build a proper sequence of events and activity timings. Hence, all systems should be verified to ensure that time synchronization technology is in use and functional.

**10.5 Secure assessment trails so they cannot be altered.**

Assessment trails help keep track of all activities and provide solid evidence of all network access attempts. If the log data is changed it can cause a serious threat to security because in case of breach of information the real data of logs would not be available and it would not be possible to catch the real culprit. Hence, this requirement of PCI-DSS maintains that assessment trails should be secured so that they cannot be altered.

**10.5.1 Limit viewing of assessment trails to those with a job-related need.**

Because assessment logs hold important information, PCI DSS requires that even access to viewing them should be restricted to authorized administrators who need this access because of job responsibility. A system should be developed so that it ensures maximum level of security of assessment trail and a possibility of only limited number of users for potential information theft.

**10.5.2 Protect Assessment Trail Files from Unauthorized Modifications**

This requirement is derived from the previous one, as 10.5.1 limits viewing access to assessment trails while this one talks about unauthorized modification to assessment trail files. Compliance to this requirement can be achieved in two steps. In first step, the organization has to prove that the assessment trail has not been access by any unauthorized personnel, so no unauthorized changes have taken place. In the second step we have to show that only unauthorized personnel accessed the assessment trail, even if a new user did so. To prove this, a report should be presented which shows which users accessed the system and also validates new entries that access the network objects.

**10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.**

Security breaches usually occur weeks or months before they are detected. It is hence recommended to daily review logs of all the system components which store, process or transmit cardholder data or that have indirectly an impact on the cardholder data. Review and check a sample of all system components and servers that carry out security functions.

**10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).**

Audit logs must be saved for a minimum time period of one year to cater for the fact that many times a security compromise is discovered quite after some time of its actual occurrence. These logs should be stored online as offline storing of logs would result in delayed availability. At least 3 months old logs should be kept somewhere where they are readily available at all times. Audit policies and procedures should be examined and personnel should be interviewed to verify that proper audit log retention policies exist, and that official procedures exist to maintain audit logs for one year along with immediately available 3 months old logs

**10.8 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.**

Personnel should be interviewed to verify that all security policies and procedures are communicated to them.