Strengthening PCI Compliance Posture with DB Audit Expert

In an attempt to protect its cardholders from identity theft VISA introduced its Cardholder Information Security Program (CISP) in June 2001. The program was intended to safeguard personally identifiable information (PII). It applied to merchants, service providers, and payment channels that maintained, collected or transmitted VISA account holder data. Other credit card companies, most notably MasterCard, followed VISA's lead and introduced similar standards.

Since that time VISA and MasterCard have collaborated with American Express, Discover and JCB to develop the Payment Card Industry Data Security Standard, otherwise known as PCI-DSS. PCI-DSS specifies a common framework on how companies handling credit card data should protect that information. PCI security is enforced through annual audits and non-compliant organizations face a broad range of penalties, including steep fines.

Database auditing is a valuable tool in securing the information infrastructure used to process and store credit card information. SoftTree Technologies' DB Audit Expert delivers essential visibility into all database activity, enabling database administrators to identify both weaknesses and successes in the systems, processes and procedures used to secure payment card industry data.

PCI-DSS Requirements and Database Auditing

PCI-DSS defines 12 requirements for protecting credit card data. The requirements apply to all system components – defined as any network component, server, application, or tool that can connect to the data. DB Audit Expert is a pragmatic solution for addressing five of the twelve PCI-DSS requirements.

PCI 1: Install and maintain a firewall configuration.

Once a best practice firewall configuration has been implemented, DB Audit Expert helps to ensure that those authorized to connect to the database through the firewall do so in a manner that is compliant with the enterprise security and policies that govern access and use of the information in the database.

PCI 3: Protect stored cardholder data

It is impossible to protect cardholder data unless you know where it is stored and what is happening to the data at all times. DB Audit Expert provides an automated search utility to enable database administrators to quickly identify databases and database tables containing PCI data.

PCI-DSS recommends the use of encryption to protect cardholder information. However, for many companies it is not practical or even possible to use encryption. In these situations compensating controls are permissible. Database auditing is a compensating control that can be used in place of encryption. DB Audit Expert also provides detailed insight into user activity affecting cardholder data.

PCI 6.3.3: Separation of duties between development, test and production environments
PCI compliance cannot be achieved without ensuring a separation of duties between production DBAs and application DBAs. DB Audit Expert helps to maintain separation between those who build and maintain database applications, those who create content and those who produce database activity reports for compliance officers and auditors.

PCI 7: Implement strong access controls
DB Audit Expert provides a comprehensive solution for managing database logins, users, security settings and permissions. Once database access controls have been implemented, database auditing helps to verify that access controls are working properly. DB Audit Expert helps track who accessed data to provide an additional layer of cardholder data security.

PCI 10: Track and monitor all access to network resources and cardholder data
Requirement 10 mandates the auditing of all accesses to cardholder data, daily review of audit logs, and the ability to reconstruct a range of events tied to cardholder information. DB Audit Expert will monitor and track all access and changes to cardholder data, including:

- Who – the username of the person who made the change
- When – the date and time of the change
- What – the name of the table and column that was changed
- Type of change (insert, update or delete)
- What it was – the data value before the change
- What it is – the data value after the change
- The source of the data change (query tool, application, etc.)
- The machine name of the user or source that made the change

Requirement 10 also mandates that the audit trails be secured, unmodified and retained for period in accordance with its effective use and legal regulations. DB Audit Expert's central repository utilizes a standard SQL database. As such, the central repository leverages the database's built-in features to manage audit trail integrity, retention and archiving.

Summary
PCI-DSS compliance is achieved via a combination of procedures, processes and technical controls. No single vendor can provide solution to address all twelve PCI-DSS requirements. Vendors can, at best, offer solutions that follow prescribed best practices, contain necessary technical controls or enable an organization to determine its compliance posture.

SoftTree Technologies' DB Audit Expert is a cost-effective, pragmatic solution to address five of the twelve PCI-DSS requirements. With DB Audit Expert organizations

can develop a database auditing infrastructure to actively audit whenever a change occurs to specified tables or fields containing payment card industry data.