PCI DSS SecureCloudDB Mapping

The following document provides a view of how SecureCloudDB either enforces, or assists in enforcing, the 12 Requirements and sub controls within the PCI-DSS compliance standard, version 3.2.1.

Importantly, SecureCloudDB fully or partially enforces all of the Requirements and sub controls which are within the intended use of the product and the scope of cloud database security.

Please note that some Requirements and sub controls, such as Requirement 7 or sub control 1.1 are outside of these parameters and, thus, not addressed. Also note that, in some cases, the capabilities of SecureCloudDB may vary depending on the level of support for an individual database.

www.SecureCloudDB.com

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

SecureCloudDB assists with this control by showing cloud databases that have weak networking controls.

1.1 Establish and implement firewall and router configuration standards that include the following:	Not applicable
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	SecureCloudDB network checks validate compliance with this requirement. Note: 1.2.1 is covered, 1.2.2 and 1.2.3 are out of scope.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	SecureCloudDB network checks validate compliance with this requirement. Note: the requirements within this section do not directly apply to a cloud deployment, and only reference on-premise systems and networking approaches. A cloud deployment achieves the overall goal of this control by using Virtual Private Cloud (VPC), or other private network solutions, depending on the cloud provider.
1.4 Install personal firewall software	Not applicable.
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	SecureCloudDB assists with this control by alerting when configurations have changed.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

SecureCloudDB checks validate compliance with this requirement, and further alerts when default users are present and/or enabled.

2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	SecureCloudDB assists with this, though no databases which are currently supported have default passwords.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	This control is the focus of all the Foundational Security rules. While ensuring that organizational policy is tailored to a given set of requirement would be up to that organization's security team, SecureCloudDB will enforce compliance with any set of configuration standards.
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.	Not applicable.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	SecureCloudDB will warn when unnecessary components are enabled.

2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	SecureCloudDB recommends countermeasures for insecure authentication and networking configurations.
2.2.4 Configure system security parameters to prevent misuse.	SecureCloudDB explicitly covers this control.
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	As noted in section 2.2.2, SecureCloudDB will assist in identifying some extraneous functionality, though this requirement is largely not applicable.
2.3 Encrypt all non-console administrative access using strong cryptography.	SecureCloudDB addresses this control directly.
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	SecureCloudDB addresses this control directly, by enumerating all databases in your environment.
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	Not applicable.
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data.	Not applicable, responsibility of cloud provider.

Requirement 3: Protect stored cardholder data.

SecureCloudDB assists with this set of controls by helping ensure that underlying encryption at rest is in place. The majority of this set of controls is not applicable.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

SecureCloudDB enforces this control by requiring secure network configuration and correct use of TLS versions and cipher suites.

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	SecureCloudDB enforces this control.
4.2 Never send unprotected PANs by enduser messaging technologies (for example, email, instant messaging, SMS, chat, etc.).	Not applicable.
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	Not applicable.

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs.

Not applicable when managed systems are evaluated.

Requirement 6: Develop and maintain secure systems and applications.

SecureCloudDB enforces this control with respect to covered databases.

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	SecureCloudDB enforces this control with respect to covered databases.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release.	SecureCloudDB enforces this control with respect to covered databases.
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle	SecureCloudDB enforces this control with respect to covered databases.

6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	SecureCloudDB will assist in enforcing this control in a future update.
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability	Not applicable.
6.4 Follow change control processes and procedures for all changes to system components.	Not applicable.
6.5 Address common coding vulnerabilities in software-development processes	Not applicable.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks	Not applicable.
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	Not applicable.

Requirement 7: Restrict access to cardholder data by business need to know.

Not applicable.

Requirement 8: Identify and authenticate access to system components.

SecureCloudDB helps enforce this control for database assets.

8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators	This control may involve some complexity, and it is common for it to be enforced at outer layers, instead of directly in a database. Several subsections are not applicable.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	Not applicable.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	Not applicable.
8.4 Document and communicate authentication policies and procedures to all users	Not applicable.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods	Not applicable.

8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access	Not applicable.
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	SecureCloudDB assists in compliance with this control through activity monitoring.
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	Not applicable.

Requirement 9: Restrict physical access to cardholder data.

Not applicable.

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

SecureCloudDB helps compliance with this control through access monitoring.

10.1 Implement audit trails to link all access to system components to each individual user.	SecureCloudDB assists in compliance with this control through activity monitoring.
10.2 Implement automated audit trails for all system components	SecureCloudDB assists in compliance with this control through activity monitoring.
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 • Failure and success • Origination • Identity of affected data	SecureCloudDB assists in compliance with this control through activity monitoring.
10.4 Using time-synchronization technology, synchronize all critical system clocks and times	Not applicable.
10.5 Secure audit trails so they cannot be altered.	SecureCloudDB assists in compliance with this control by sending logging information to an external system, which if properly configured, would comply with this control.

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	SecureCloudDB assists in compliance with this control through activity monitoring.
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).	SecureCloudDB may assist in enforcing this control in a future update.
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	SecureCloudDB access monitoring assists in complying with this control.
10.9 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.	Not applicable.

Requirement 11: Regularly test security systems and processes.

SecureCloudDB assists in some aspects of compliance with these controls.

11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	Not applicable.
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	SecureCloudDB Foundational security checks enforces compliance with this control for database assets.
11.3 Implement a methodology for penetration testing	Not applicable.
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network.	SecureCloudDB access monitoring assists in compliance with this control.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	SecureCloudDB access monitoring assists in compliance with this control.
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	Not applicable.

Requirement 12: Maintain a policy that addresses information security for all personnel.

Not applicable.