

Req't.	Summary Description	Guardium PCI DSS Capabilities
2	<b>Do not use vendor defaults for system passwords</b> <ul style="list-style-type: none"> <li>• Configure system parameters to prevent misuse</li> <li>• Encrypt non-console admin access</li> </ul>	<b>Comprehensive suite of DBMS-specific tests based on industry standards (CIS, STIG)</b> <ul style="list-style-type: none"> <li>• Checks for default passwords, misconfigured accounts, privileges, etc.</li> <li>• Tracks and audits usage and alerts on misuse</li> <li>• Locks configurations after vulnerabilities remediated</li> <li>• Monitors encrypted traffic (Oracle ASO, SSL, etc.)</li> </ul>
3	<b>Protect stored cardholder data</b>	<b>Real-time database leak prevention</b> <ul style="list-style-type: none"> <li>• Auto-discovers and classifies stored data; identifies sensitive data in query result stream</li> <li>• Continuous, real-time policy-based monitoring with proactive security (alerts, blocking)</li> <li>• Compensating control for column-level encryption</li> </ul>
6	<b>Maintain secure systems</b> <ul style="list-style-type: none"> <li>• Establish a process to identify security vulnerabilities</li> <li>• Follow change control procedures for all configuration changes</li> <li>• Separation of duties (development, test and production)</li> </ul>	<b>Centralized vulnerability and configuration assessment</b> <ul style="list-style-type: none"> <li>• Ensures all current patches are applied and vulnerabilities identified; provides "virtual patching"</li> <li>• Alerts on all configuration changes</li> <li>• Enforces separation of duties (SOD) with real-time alerting and granular access controls</li> </ul>
7	<b>Restrict access to cardholder data</b>	<b>Proactive, real-time access control (independent of native DBMS controls)</b> <ul style="list-style-type: none"> <li>• Blocks any unauthorized user, including DBAs and system administrators, from accessing cardholder data</li> <li>• Policies defined by source IP or application, OS or DB user, time, SQL command, object, etc.</li> <li>• Compensating control for unsegmented networks</li> </ul>
8	<b>Assign a unique ID to each person with computer access</b> <ul style="list-style-type: none"> <li>• Enforce password policies</li> <li>• Limit repeated access attempts</li> </ul>	<b>Complements native DBMS controls with external, cross-DBMS controls</b> <ul style="list-style-type: none"> <li>• Alerts on credential sharing, failed logins, account creation, privilege escalation</li> <li>• Verifies password policies are enforced; locks accounts or terminates sessions</li> </ul>
10	<b>Track and monitor access to cardholder data</b>	<b>Continuous, granular auditing with scalable architecture to handle high transaction volumes</b> <ul style="list-style-type: none"> <li>• Fine-grained audit trail of all database activities (SELECTs, DDL, DML, DCL, logins, etc.)</li> <li>• Does not rely on native trace or audit logs: has minimal performance impact; enforces separation of duties</li> <li>• Tracks all network and local connections, including direct access by DBAs (shared memory, etc.)</li> <li>• Audit information stored securely in separate appliance to prevent anti-forensics/tampering</li> <li>• Identifies fraud by resolving end-user IDs in multi-tier, connection-pooling applications such as SAP, PeopleSoft, etc.</li> <li>• Integrates with LDAP, IAM, SIEM, change management, CMDBs, McAfee ePO, etc.</li> <li>• Compliance workflow automation (electronic sign-offs, escalations) demonstrates proactive oversight process</li> <li>• PCI Accelerator provides pre-configured reports based on best practices</li> </ul>
11	<b>Regularly test security systems and processes</b> <ul style="list-style-type: none"> <li>• Run internal and external vulnerability scans</li> <li>• Deploy integrity monitoring to detect modification of critical system files</li> </ul>	<b>Integrated vulnerability scanning, file integrity monitoring and behavioral vulnerability testing</b> <ul style="list-style-type: none"> <li>• Includes hundreds of pre-configured vulnerability tests for all major DBMS/OS combinations</li> <li>• Tracks changes to database configuration files and other external objects such as environment/registry variables, executables, scripts and OS files</li> </ul>
12	<b>Maintain an Information Security Policy</b> <ul style="list-style-type: none"> <li>• Monitor and analyze security alerts and distribute to appropriate personnel</li> <li>• Monitor and control all access to data</li> </ul>	<b>Robust automated controls for enforcing information security policies</b> <ul style="list-style-type: none"> <li>• Real-time alerts, correlation alerts, centralized aggregation of all audit data, SIEM integration</li> <li>• Automated sign-offs demonstrate formal oversight process</li> <li>• 100% visibility and control over all database transactions (with optional blocking)</li> </ul>