Oracle Solutions for Payment Card Industry Compliance

An Oracle White Paper
December 2008
EXECUTIVE OVERVIEW
The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of specific credit card holder protection regulations and guidance to combat identity theft. The PCI DSS grew out of common requirements between Visa’s security initiative, the Cardholder Information Security Program (CISP), and MasterCard’s Site Data Protection (SDP) program. The PCI Security Council, an industry group, manages the PCI DSS, which all major credit card companies have ratified.

The PCI DSS security measures require that a Qualified Security Assessor (the PCI Security Council identifies appropriate parties) assess all merchants and service providers for key information security best practices. And, depending on the size of the merchant or service provider, a Qualified Security Assessor must also evaluate (for security vulnerabilities) all merchant and service provider systems involved in the handling or processing of cardholder information. Further, PCI assesses penalties and fees to any organization that is found to be deficient in securing cardholder data.

Oracle is uniquely suited to provide software and services to help companies comply with the PCI DSS requirements. Oracle’s Defense-In-Depth, an infrastructure-based, holistic, enterprise-wide approach to security, can help retailers address the need for PCI compliance. In fact, Oracle specifically designed its applications, middleware, and database products to secure information; these data protection capabilities can be effectively applied to point-of-sale (POS), back office, and enterprise environments. According to the AMR Research: Using CobiT To Fill Gaps in Regulatory Security Requirements, a holistic approach to security will result in higher security and better compliance for less cost.

INTRODUCTION—WHAT IS PCI?
When Visa USA first mandated the CISP in June 2001, the company intention was to protect Visa cardholder data to promote consumer confidence in conducting business electronically. Now, in 2007, VISA verifies that merchants and service providers maintain the highest information security standards. To maintain these standards, Visa requires all merchants and service providers that store, process, or transmit Visa cardholder data (via any payment channel—retail, mail/telephone order, or e-commerce) to comply with CISP.
The MasterCard SDP Program is a proactive process for MasterCard and its acquiring members (a financial institution that screens and accepts merchants into its bankcard program, processes transactions, and completes financial settlement for MasterCard) to help merchants, service providers, third-party processors, and data storage entities protect themselves and the overall payment system against the threat of compromise. The SDP Program identifies vulnerabilities in processes, procedures, and Web applications. Additionally, MasterCard’s program addresses the security issues that online merchants and their acquiring banks face in the virtual world as well as concerns arising from these issues, such as Internet fraud, chargebacks, damage to brand image, consumer information safety and privacy, and the cost of replacing stolen account numbers.

If merchants and service providers adhere to the PCI DSS—a single approach to safeguarding sensitive data for all card brands, then those merchants and service providers achieve compliance with the Visa and/or MasterCard programs. In fact, the PCI DSS is a result of the collaboration between all major credit card companies (including Visa, MasterCard, JCB, American Express, and Discover) that designed the PCI DSS to establish industry-wide security requirements. Using the PCI DSS as the framework, these credit card company security programs provide the tools and measurements needed to protect against cardholder data exposure and compromise.

In the case of a compromise, companies that are part of the PCI Security Council, such as MasterCard and Visa, will fully exempt an acquirer from data-security-related non-compliance assessments, investigative costs, and issuer reimbursement costs if the compromised entity is found to have been both compliant with the PCI DSS and registered as compliant at the time of the compromise.

**PCI REQUIREMENTS**

According to the Version 1.1 Release, September 2006¹, the PCI DSS has six control objectives that are broken up into 12 high-level requirements:

1. **Build and Maintain a Secure Network.**
   - **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data.
   - **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters.

2. **Protect Cardholder Data.**
   - **Requirement 3:** Protect stored cardholder data.
   - **Requirement 4:** Encrypt transmission of cardholder data across open, public networks.

3. **Maintain a Vulnerability Management Program.**
   - **Requirement 5:** Use and regularly update anti-virus software.
   - **Requirement 6:** Develop and maintain secure systems and applications.

¹ Source: https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf
4. Implement Strong Access Control Measures.
   Requirement 7: Restrict access to cardholder data by business need-to-know.
   Requirement 8: Assign a unique ID to each person with computer access.
   Requirement 9: Restrict physical access to cardholder data.

5. Regularly Monitor and Test Networks.
   Requirement 10: Track and monitor all access to network resources and cardholder data.
   Requirement 11: Regularly test security systems and processes.

   Requirement 12: Maintain a policy that addresses information security.

RECOMMENDED APPROACH

Many merchants pursue point solutions for PCI DSS compliance, thereby attempting to secure different elements of their environment individually, yet achieve compliance overall. This approach, however, tends to be more expensive and less effective than alternative approaches. Vendor marketing should not fool merchants. Security is not the same as compliance.

Even if each system is individually secured, the security models of each point solution within a merchant’s environment must integrate to achieve compliance. In fact, tying these systems together usually requires a risky and highly expensive integration project, which is an ineffective way of closing all the gaps. A merchant should always be wary of deploying a point solution product that addresses a specific security issue, as this will NOT achieve compliance. Instead, an organization must coordinate security with compliance and business process activities to achieve a common, unified security infrastructure.

Coordinating security with compliance and business process activities is the best practice for securing cardholder data, and this starts with a “Defense-In-Depth” approach. Data must be secured at every tier of an enterprise and in every space in between, from point-of-sale through in-store processing and all the way to back-end applications, data warehouses, and backups.

The most secure, efficient, and cost-effective strategy to achieve a Defense-In-Depth posture is to implement a unified security infrastructure or a highly available, scalable, and extensive infrastructure that every system, data store, device, and application in the network can leverage with no gaps or points of failure. Additionally, a unified security infrastructure provides a single model for control and visibility of an environment, including consistent policies around authentication, encryption, access control, and information lifecycle management. A single model for control and visibility of the environment through a unified security infrastructure makes PCI DSS compliance easily attainable and also provides a foundation for meeting other regulatory mandates, such as the Financial Institutions Examination Council (FFIEC), Gramm-Leach-Bliley, and Sarbanes-Oxley.
In addition to low cost and low-risk regulatory compliance, a unified security infrastructure also enables additional business benefits including:

- **Greater Business Agility.** Ordinarily, organizations spend a great deal of time and expense (analysts estimate up to 30 percent of development lifecycle resources) redundantly coding, recoding, and configuring security within each application and system. When these systems and applications leverage a centralized security infrastructure, merchants can adapt to changing processes or threats, as well as respond to changing business environments more quickly and with less expense.

- **Additional Revenue Channels.** Deploying revenue-generating services outside the corporate perimeter is an enormous risk. When leveraging a unified security infrastructure, merchants can build these revenue channels on top of a reliable security service, thereby mitigating risk and lowering costs.

- **Lower Operational Expenses.** Numerous organizations have found that a unified security infrastructure provides user and information lifecycle management services that enable automation of processes, provide efficiencies, and produce gains that have an impact on the bottom line.

**WHY ORACLE?**

Oracle offers the most complete solution, with unique capabilities that address PCI requirements while significantly reducing your time-to-value and cost of compliance. With Oracle solution, organizations will:

- Ensure sustainable and automated compliance with advanced technologies
- Optimize enterprise security and user productivity with comprehensive integrated solutions
- Rely on proven, best-in-class solutions that are hot-pluggable
- Leverage industry leadership with specific expertise

**Sustainable Compliance**

Here are some of the unique capabilities of Oracle products that help enforce sustainable compliance: Oracle Database Vault prevents even privileged DBAs from accessing sensitive data – the first and only privileged database user access control solution in the industry. Oracle Identity Management automates key compliance processes such as Attestation, enforcement of Separation of Duties, and audit reporting. Oracle ASO transparently encrypts data on disk and on the network to protect consumer data, while requiring no application changes whatsoever. Oracle Governance Risk and Compliance Manager (GRCM) automates enforcement and management of compliance processes and IT controls thereby providing sustained compliance. Oracle Enterprise Manager (EM) offers
deep diagnostics and out-of-box remediation for scalable results. Integration among Oracle Identity Management Suite, Database Security, GRCM and EM solutions ensure consolidated, tamper-proof audit data and stricter access controls. Additionally, customizable and out of the box reports make it easier to obtain a holistic view of enterprise data access.

Security with Productivity

Oracle’s comprehensive integrated solutions, spanning database, middleware, and enterprise applications optimize enterprise security and user productivity. Oracle’s leadership in Database, ERP, and CRM software ideally positions it to offer the most complete PCI solution. Point solutions end up costing more, are hard to integrate and scale. Often those leave security gaps as there is no centralized mgmt or reporting. End-to-end Oracle solution offers lowest TCO and comprehensive security. Organizations can leverage Oracle solutions to not only meet their compliance needs but also to centralize and streamline IT infrastructure, user, data, applications and identity management

Proven, Best in Class

Oracle solutions are built on the pillars of open standards. Oracle is committed to interoperability and continues to add support for new environments. Oracle solutions are interoperable with all leading applications, app servers, operating systems, directories, portals, and host systems

Oracle has proven best-in-class solutions with Oracle products regularly featured as leaders on Gartner Magic Quadrant reports and other industry studies. Leading organizations rely on Oracle for their security and compliance needs.

Industry Leadership

Oracle has invested heavily in developing deep, industry specific experience within retail and financial services. This experience combined with comprehensive software building blocks based on open standards enables Oracle to unify security from the point-of-sale all the way back to the data warehouse, with low integration costs and no gaps, even in a heterogeneous environment. In other words, thanks to the interoperable nature of the unified security infrastructure, organizations can still realize significant value even if they are not using Oracle Retail Applications, Oracle Fusion Middleware, or Oracle Database products.

THE ORACLE SOLUTION

The ways in which Oracle helps to satisfy the 12 PCI DSS requirements, previously cited, follow below. Each product is part of Oracle’s unified security infrastructure:

- **Requirement 1: Install and maintain a firewall configuration to protect cardholder data.** Under this, sub-requirement 1.2 further
states: “Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.”

One concern on the part of merchants is what to do about traffic involving necessary protocols that may come from “untrusted” sources.

Oracle helps to address this concern as follows:

- Oracle Database Vault has the capabilities via Rules and Factors to deny or limit database access from IP address ranges that are deemed “untrusted.”

- Oracle Audit Vault is a tamper-proof, write-once database that enables the aggregation and centralization of audit logs, including firewall logs, from wherever they are generated.

- The Oracle Virtual Directory (OVD) can be used to act as a directory firewall, in particular for client applications that are located in network’s DMZ and need to access directory data within the corporate network. Organizations can also use OVD to provide Denial of Service (DoS) protection and additional layers of access control security such as restricting types of queries, hiding attributes at the source layer (beyond what normal Access Control Lists can do) and encrypting attribute values on the fly. This way they can provide “defense in depth” to their directory architecture as well as their database.

- Oracle Enterprise Manager features plug-ins for third party firewalls that enables the management and configuration of firewall installations at remote sites.

**Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.** Sub-requirement 2.1 deals with vendor-supplied defaults, and sub-requirement 2.3 requires encryption of all non-console admin access. In the environment, do system accounts have default passwords? How strong are passwords on system accounts? Does administrator access require encryption?

Oracle helps to resolve these questions as follows:

- When installing the Oracle Database 10g, the Database Configuration Assistant locks and expires user accounts by default, as long as one includes the Database Configuration Assistant in the Database install. This allows organizations to activate only those accounts that need to be utilized, thereby practicing a “least privilege” model.
- Oracle Enterprise Manager provides the ongoing, necessary checks of default passwords.
- Oracle Database Vault implements strong password policies and addresses concerns over unauthorized system account access.
- Identity Administration features in Oracle Identity Manager (OIM) and Oracle Access Manager (OAM) allow setting up complex password policies for user accounts in various applications.
- The following features in various Oracle Identity Management products eliminate the pain of maintaining multiple passwords across enterprise applications.
  - OIM provides the password synchronization features so that a validated password (that satisfies all password complexity rules) may be propagated to all enterprise wide applications.
  - OAM and Oracle Enterprise Single Sign-on may be used to implement enterprise wide sign on for all web and desktop applications. When applications are single sign-on enabled, the password is maintained in a single identity repository (generally LDAP) rather than across different application’s identity repositories.
  - Both OIM as well as OAM allow enforcement of password change after first login (new registered user) and helpdesk assisted password reset.
  - OAM also allow runtime enforcement of certain password policies while using single-sign-on to various enterprise applications. As an example, a runtime enforcement policy may specify that the user’s account may be locked after 5 consecutive failed login attempts.
  - Oracle Advanced Security optionally encrypts all traffic to and from the Oracle Database.

**Requirement 3: Protect stored cardholder data.** Requirement 3 deals with cardholder data “at rest” or in storage. A merchant environment might store cardholder data in several places: on a point-of-sale (POS) device, in an in-store transaction processing system, at a corporate data warehouse, or on a backup tape. In addition, sub-requirement 3.2.1 explicitly prohibits storage of “the full contents of any track from the magnetic stripe,” and sub-requirement 3.3 mandates that a merchant must always mask the cardholder’s Primary Account Number (PAN) unless a person or system has a legitimate need to know.
Data Lifecycle Protection is an important component of an overall compliance strategy. Important steps include: reviewing data classification and data retention requirements; understanding where the cardholder data resides; and establishing proper protective controls wherever cardholder data resides.

Oracle assists with addressing requirement 3, as well as the steps within Data Lifecycle Protection, as follows:

- Transparent Data Encryption provides encryption of sensitive data on disk or backup media, transparent to applications and users; key management is automated, application don't need modifications and developers can focus on business logic without taking a crash-course in encryption and key-management.

- Oracle Secure Backup fully encrypts backups to tape to protect against loss or theft of the tape backups.

- OVD Mapping framework can be used to prevent the display of sensitive information such as PAN when it is being retrieved.

- OIM allows encryption of sensitive user attributes like PANs so that even most privileged users (other than Oracle Identity Manager application) like DBAs may not access it.

- Oracle Internet Directory (OID), Oracle’s LDAP v3 compliant directory product, allows usage of Oracle Database Vault for defining data access realms on Oracle Internet Directory data that is stored in Oracle DB. By using Database Vault realms, organizations can ensure that even most privileged users are not able to select, insert, update or delete the most sensitive data. Additionally OID allows use of Transparent Data Encryption (TDE) features of Oracle DB to provide secure storage of sensitive data. TDE ensures that the data may not be accessed directly from backups, tape archives or data files. Virtual Private Database is a feature in the Oracle Database that provides row and/or column-level access controls; certain columns can be defined as ‘sensitive’, and some or all rows of these columns are displayed empty, depending on the user’s authorizations.

- Oracle Retail Applications implements best practices by providing encryption of cardholder data on the POS device and never stores full-track data.

**Requirement 4: Encrypt transmission of cardholder data across open, public networks.** This requirement deals with cardholder data “in transit” as it traverses wired and wireless networks, within a transaction.

Oracle’s technology capabilities include the following:
o Oracle Advanced Security Option can encrypt incoming and outgoing Oracle SQL traffic, whether the connection is from an application server executing a transaction or from a DBA connecting into the database using administrative tools.

o Oracle Adaptive Access Manager uses the following encryption methods to ensure secure encrypted transmission of cardholder data across open, public networks.

  o An encryption method that foils mouse click loggers by “jittering” our device image for each new session
  
  o A method for randomizing the file size of our device image for each new session, to foil automated image-based dictionary attacks
  
  o Randomization of measurable properties (size, position, checksum, relative values etc) in each session to protect against software-based automated OCR (image capture) attacks
  
  o An OTP-like encryption method which ensures data corresponding behind the image (for example numeric data on a PinPad) is randomized every time it is transmitted to the server to secure data over the wire. This is referred to as “data encryption”

Using Oracle Adaptive Access Manager, a second encryption method which ensures the entire virtual authentication device image is recompiled, in unique fashion, on the server, for each session to protect against software-based automated OCR (image capture) based attacks. This is referred to as “checksum encryption”

o Oracle Fusion Middleware also supports wireless security standard protocols.

• **Requirement 5: Use and regularly update anti-virus software.**

  This requirement primarily deals with “best practices” around scanning and protecting against viruses. Sub-requirement 5.1 states: “Deploy anti-virus software on all systems commonly affected by viruses.”

  But how does an organization confirm deployment of anti-virus software on numerous systems? How does an organization analyze and secure anti-virus logs? Although anti-virus software is not Oracle’s core competency, secure deployment of critical software to distributed systems is a core competency.

  Oracle’s technology capabilities include the following:
Oracle Enterprise Manager can build a “gold image” to provision new systems with an operating system, anti-virus software, and other software.

Oracle Audit Vault is a tamper-proof, write-once database that enables retailers to aggregate and centralize distributed audit logs, including anti-virus logs.

- **Requirement 6: Develop and maintain secure systems and applications.** This requirement brings a number of concerns to light.

Sub-requirement 6.1 mandates that organizations deploy the most secure patches. While this is indeed important, a best practice is for an organization to use latest version of software as well. Older versions of POS applications write track data, which is forbidden in sub-requirement 3.2.1. Also, newer versions of operating software and server software address existing vulnerabilities in older software versions.

Monitoring custom applications is a concern. Does the organization practice secure coding? Sub-requirement 6.3 mentions the software design life cycle (SDLC). Two best practices in the SDLC are to incorporate security at design time and to leverage existing services rather than to duplicate effort. Even when organizations practice secure coding, they must still closely monitor applications. Does the organization have a good change management process in place? Sub-requirement 6.4 addresses this concern by stating: “A unified security infrastructure leverages both coding and change management best practices.”

Oracle addresses many of these concerns as follows:

- Oracle Enterprise Manager enables patch and version management and deployment, addressing sub-requirement 6.1.

- Oracle Internals Control Manager addresses any vulnerability that a configuration change in an application might introduce.

- Oracle Change Management Pack tackles sub-requirement 6.4.

- Oracle is very involved in the Open Web Application Security Project (OWASP), an organization that promotes secure Web coding and is specifically mentioned in sub-requirement 6.5. Oracle also practices internal secure development when developing Oracle solutions.

- **Requirement 7: Restrict access to cardholder data by business need-to-know.** This requirement primarily deals with making sure only authorized users get access to data on a “need to know” basis. As a result, organizations need more efficient application controls. If a
standard application control method is not in place, an inconsistency may exist, which exposes an application to unauthorized access.

Another concern for merchants is the need for access control where data resides. As previously mentioned, administrators can access data directly from administrative tools, so an organization needs to adequately protect data at its source. Auditors immediately look for rogue or orphaned user accounts, as these extraneous accounts that are left active can lead to unnecessary or illicit access.

Oracle addresses the requirements outlined in requirement 7 as follows:

- **Oracle Access Manager** provides authentication and authorization services for user and system access to applications, transactions, and other resources.
- **Oracle Identity Manager** automates onboarding and offboarding of users, reducing the incidence of dormant or unauthorized accounts. It supports “least privilege” and “need to know” principles natively. Oracle Identity Manager also provides role consistency so that (a) a user’s role is consistently applied in all systems, and (b) if that role changes, the user’s access will instantly change accordingly in all systems. Additionally, OIM allows organizations to define “Explicit Deny” policies. As the name suggests, these types of policies explicitly mandate what level of specific users or groups should not have particular access. These policies support the implementation of a mechanism where access to critical information is denied by default.
- **Oracle Enterprise User Security** can be used to provide centralized role management for Oracle databases – thus simplifying the management of segregation of duties. EUS works with/requires Oracle Directory Services. OIM can be then used to facilitate LDAP Groups.
- **Oracle Database Vault** provides strong internal controls and can provide separation of duties in the Oracle Database, effectively preventing database administrators from having unfettered access to data. Oracle Label Security provides fine-grained access control and provides row-level security for data out-of-the-box.
- **An important part of “Defense In-Depth”** is preserving the identity of a user throughout a system transaction and implementing controls at all layers. Oracle Access Manager provides identity preservation from the perimeter (e.g., POS, employee workstation, customer Web browser) to the middle tier,
and Oracle Proxy Authentication and Client Identifiers provide identity preservation from the middle tier to the data level.

• **Requirement 8: Assign a unique ID to each person with computer access.** This requirement refers to providing each user with an ID that is unique and cannot be shared with any other user.

How does an organization uniquely identify a user and initially provision the user into systems? Organizations are often unsure of how to generate a unique ID and provide single sign-on for users, unify and rationalize cardholder data from multiple repositories, increase the quality of cardholder data, and streamline application development.

How can the right level of authentication be provided? Sub-requirement 8.3 is specific in that two-factor authentication (something you have and something you know) is required for remote access. Other instances where access is granted to high-value data may also merit that level of authentication.

How does a retailer better control onboarding and offboarding? Getting users efficiently and securely in and out of systems is critical. Sub-requirement 8.5 enumerates certain session management specifications and password management policies around password composition and expiration.

Oracle technology addresses requirement 8 through the following products:

- Oracle Identity Manager automates provisioning and de-provisioning as well as the generation and propagation of unique IDs.
- Oracle Virtual Directory provides a single standards-based interface to cardholder data in distributed data stores.
- Oracle Enterprise User Security provides a single authenticator and role repository for a distributed Oracle Database environment.
- Oracle Access Manager provides two-factor authentication and Oracle's Single Sign-On in an application environment. The technology also provides session and password management policy definition and enforcement.

• **Requirement 9: Restrict physical access to cardholder data.**

Physical access control requires a combination of access policy decision-making and access policy enforcement. An electronic door lock associated with a badging system usually provides physical access policy enforcement. This system identifies the person who is
attempting access and makes a decision as to whether or not to grant access and unlock the door.

The following products address requirement 9:

- **Oracle Identity Manager** provisions a user’s role or other information to a physical security system so that the physical security system can determine whether to grant access. This means that if an employee is transferred from a position where the employee needs access to a position where the employee does not, the physical security systems can instantly enforce that change.

- In some cases, physical security systems themselves can leverage external security services like Oracle’s unified security infrastructure. In this case, Oracle Access Manager provides real-time access policy decisions based on the most up-to-date and accurate identity data. Both physical security systems and a security infrastructure achieve instant alignment between physical and logical security.

- With the ability to develop system monitoring plug-ins for networked devices, the status of your network-accessible physical security controls can be monitored with Oracle Enterprise Manager.

- **Requirement 10: Track and monitor all access to network resources and cardholder data.** This requirement includes the following:

  - Systems monitoring for intrusions and anomalies. Establishing preventive controls is only part of the solution; detective controls are important to catch unauthorized or malicious access as it happens.

  - Implementation of reporting and analysis tools. If unauthorized access occurs, an organization needs tools that can provide forensics for possible prosecution. Also, most regulations require extensive reporting. Analysis tools can add additional value around items like usage trends for cross-marketing opportunities.

  - Centralization and securing of audit data. Sub-requirement 10.5 addresses the securing of audits, but aggregation and centralization of audits is most efficient for getting value from audit logs.

  - Data analysis. How do retailers analyze all this data? Sub-requirement 10.6 specifies: “Review logs for all system components at least daily.” How do retailers implement alerts? Having useful alerts in place as a detective method is an important part of the overall audit strategy.
Access monitoring. How do retailers monitor who has access to what? Having reporting facilities in place to understand all access policies is critical. How does an organization secure audit trails? This is specified in sub-requirement 10.5.

Oracle addresses many of these concerns as follows:

- Oracle Database has fine-grained auditing that can key off certain data and provide alerts when unauthorized access or changes occur.

- Oracle Identity Manager provides reports that show those to whom the organization has given access rights across the enterprise.

- Oracle Access Manager provides reports that show those to whom the organization has given application access.

- Oracle Audit Vault provides aggregation and centralization of distributed audit logs and establishes controls that enable tamper-proof audits.

- Oracle Adaptive Access Manager harnesses the data captured by the Tracker system — data on user location, session activity and more — and makes this data available for risk analysis.

- Oracle Adaptive Access Manager’s Risk Analyzer can be used to detect and confirm fraudulent patterns in users historical access activity and audit data. It can be used to detect fraudulent activity, high-risk transactions and patterns and behaviors in user’s access activity. The reporting and dashboard engines further provide persona-specific views of the risk analysis including geographical, risk-type and other drill downs.

- Oracle Analytics provide tools to get valuable reports out of raw audit data. Oracle Enterprise Manager features Enterprise Security Advisor: A single console to monitor, inspect and remediate Security violations. It gives Compliance score, flux and lists the targets that are most vulnerable. Monitoring Templates enable you to easily standardize best practice monitoring settings across your managed targets. Once a Monitoring Template has been defined and applied to your targets, you can generate on-demand or periodic diff reports to easily identify targets that are not in compliance with the Monitoring Template settings. Bringing these targets back to compliance is easily accomplished with a single button click

- **Requirement 11: Regularly test security systems and processes.**

  How do retailers test systems for security? Determining if a system is secure or not is often a difficult task. Too often, a breach in the system is the only indicator that a system had vulnerability. Thorough testing of security in systems is pivotal to avoiding breaches.
Organizations must ask: Is our extended enterprise (storefront, back office, corporate systems, etc.) really compliant? Organizations should have tools and methods to quantify the degree of compliance; they do not want to wait for an outside assessor to determine if they are compliant. Organizations should also perform internal analysis prior to an outside assessment to reduce the time and expense of the audit process and remediation required as a result of an audit.

Oracle assists organizations meet requirement 11 as follows:

- With Oracle Governance, Risk and Compliance Manager (GRC Manager), a company can perform efficient internal controls testing that results in a higher certainty of risk assessment.
- Oracle Identity Manager improves regulatory compliance by providing a granular attestation process whereby managers and administrators can substantiate the correctness of policies and access rights.
- Oracle Consulting can provide best practices around security policy, monitoring, and testing.
- Oracle partners who are a Qualified Security Assessor (like Protiviti) are uniquely able to provide guidance to help an organization comply with the PCI DSS requirements.

**Requirement 12: Maintain a policy that addresses information security.**

Security is 80 percent people and process and 20 percent technology. Organizations must establish proper policies and procedures and train people to be aware of and adhere to the proper policies and procedures. Sub-requirement 12.6 specifically describes the best practices of internally training staff on security policies. Sub-requirement 12.7 acknowledges the human element in security, mandating organizations to: “Screen potential employees to minimize the risk of attacks from internal sources.”

An organization should develop processes that facilitate adherence to policies. And, leveraging technologies can help an organization create effective policies.

Oracle assists organizations meet requirement 12 as follows:

- Periodic review and certification of identity data extends the reactive detective mechanism and allows a organization to implement it in a proactive manner. The process of authorizing established internal controls, processes, policies, programs, and data, is commonly referred to as “Attestation”. OIM attestation engine allows creation of attestation processes and configuring their schedule. The reviewers can be notified via email when an attestation process kicks off. OIM provides full entitlement data (who has what) including resources where users have access, as well as their fine-grained entitlements in each of the resources. OIM
further allows automation of triggering of remediation or corrective action workflows based on attestation outcome.

- Oracle partners like Protiviti are extremely experienced in developing security policies specific to PCI compliance.
- Oracle Consulting has expertise with security policy best practices for compliance.
- Oracle Enterprise Manager helps to enforce policies by providing visibility into users’ activities.
CONCLUSION

To achieve PCI compliance, an organization must consider the overall business impact, including total cost of ownership, the ability to enhance business agility, and the opportunity to build new revenue streams and drive down operating expenses. The ideal PCI compliance approach establishes a unified security infrastructure that includes integrated capabilities, the management of sensitive personal or credit information, access control policies and enforcement, vulnerability assessment, configuration management, patch management, remediation, reporting, and monitoring. Moreover, the ideal compliance approach integrates seamlessly with existing systems, including both internal systems and third-party technologies that verifiers use.

For more information on Oracle Security Solutions, visit www.oracle.com/security