Modern Compliance Solutions

Simple. Automated. Affordable.

SELECTING FOUNDATIONAL CONTROLS MAKES PCI-DSS COMPLIANCE EASIER

By:

Steven Marco and Joseph Grettenberger
Modern Compliance Solutions

Commissioned by:

DELL Software

Table of Contents

Part 1 – Updates to Regulations and IT Security Compliance Implications

With the current information security challenges facing almost all organizations and the risk of being another front page news story, information risk and IT security should not only be on the agenda of just about every corporate risk program, but they should be in sync. Sadly, such is often not the case. Even today, compliance mandates frequently drive, rather than inform, an organization's approach to enterprise-wide IT control selection and, consequentially its information security baseline. Meanwhile, information risks confirmed from actual security incidents are being addressed by those on the front line. Inevitably, three groups - risk management, IT security, and compliance - get involved when reacting to news stories. Yet, barring such an event, scarce resources, company culture, organizational misalignment and a host of other factors often keep these groups from comparing notes. The stark reality is that the job of selecting and approving the adoption of IT Security controls for many organizations has been left to misguided reactions. The result is that prioritizing the process of monitoring and re-assessing IT controls in light of actual risk is most often done in a firefighting or ad hoc manner. The idea of selecting key, foundational, high performance controls by pointing to carefully-considered corporate risk that is informed by a well-performed risk analysis still seems to be the exception rather than the rule across virtually all industries. Nevertheless, different approaches to IT security, if taken from what's been proven in the industry, are not necessarily bad, because whether from a risk program or a compliance mandate, smart IT security has become a survival issue.

A key component of regulatory compliance these days is the demonstration of appropriate IT-related internal controls that mitigate fraud risk and the implementation of necessary safeguards for legally protected information that is stored and transmitted in electronic form. Naturally, this requirement for demonstration of IT compliance also applies to the users of systems accessing this information. This paper addresses this area of IT Security compliance from an auditor's perspective for PCI DSS compliance mandates in the U.S.[1] It should be noted that for the majority of companies where one or more of these mandates apply, each represents only a portion of the organization's total scope of compliance obligations.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry (PCI) Data Security Standard (DSS) was originally released in 2004 as a cooperative effort between Visa and MasterCard to secure payment cardholder information. Two years later, the PCI Security Standards Council (SSC), an independent organization of 5 payment brands (which included Visa and MasterCard) announced its role as maintainer of the DSS and introduced version 1.1 on September 7, 2006. More recently, on November 7, 2013, the PCI SSC, which now facilitates a global forum of more than 650 participating organizations, published version 3.0 of the DSS. All PCI merchants must be compliance with version 3.0 by January 1, 2015.

1 This paper addresses PCI-DSS which is only a sample of compliance mandates that include significant IT safeguard requirements.

The intent of the PCI DSS is to minimize payment card fraud by enforcing good data security practices.

While a relative newcomer to the IT compliance scene, the PCI DSS is one of the most extensive set of rules facing organizations. Its reach is extensive: virtually any organization accepting, storing, processing or transmitting payment card data (i.e., data from credit and debit cards) is considered a PCI "merchant" and is required to comply.

PCI DSS control objectives include:

1. Build and maintain a secure network and systems
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

All founding payment brand members of the PCI SSC, which includes Visa International, MasterCard Worldwide, American Express, Discover Financial Services and JCB International, have not only embraced the standard, but are ultimately responsible for enforcing it. All banks and financial institutions that process the cards' payment transactions are likewise responsible for ensuring their merchants meet the standard. Penalties for failing to comply can be severe.

As an example of what organizations must do to comply, PCI DSS Requirement 10 emphasizes the need for organizations to employ logging and monitoring controls: "Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs."

Part 2: Introducing Dell's GRC Product Suite: ChangeAuditor, InTrust, Enterprise Reporter and the Dell Knowledge Portal

Dell GRC Product Suite

With the proliferation of information security threats mixed with the complexity of compliance mandates, organizations today need as much compliance automation they can get. The Dell GRC Product Suite helps organizations automate many of the assurance safeguards required by today's IT security mandates while also providing foundational IT security measures. For example, the Dell GRC Product Suite addresses IT general controls (ITGCs) for 6 of the 12 PCI DSS requirements. Monitoring primary databases of protected information is not enough to safeguard that information. The support systems (e.g. email, file servers, Active Directory) that

make up the environment outside the primary database often store protected information and related access controls making them additional components of a risk analysis.

The Dell GRC Product Suite enables organizations to monitor, perform self-audits, and respond to inquiries with reports that demonstrate historical compliance with many information system components of regulatory compliance security policies and procedures. In addition, the Dell GRC Product Suite can report on suspicious activities such as identifying unlocked user accounts and activity for accounts of terminated and transferred personnel.

These tools provide separate databases and a variety of reports that can substantiate evidence of policy violations when personnel sanctions related to the security of information systems need to be applied. In short, The Dell GRC Product Suite is designed to continuously monitor, evaluate and assess the IT general control areas of an organization's system of internal control. The tools equip organizations to adopt robust continuous auditing and monitoring practices that augment and to some extent preempt standard network vulnerability scanning practices.

While not a replacement for network vulnerability tools, when regularly used as part of a continuous monitoring program, Intrust, ChangeAuditor, and Enterprise Reporter can discover a host of information system vulnerabilities (e.g. outdated patch levels, unauthorized ports, protocols, and services) before network vulnerability scanning tools and technical surveillance countermeasure surveys can discover them.

By enabling the assurance functions of real-time audits, continuous monitoring and the generation of information system documentation for discrete environments, the Dell GRC Product Suite helps organizations not only watch their production operating environments but monitor critical controls in security architectures that are anticipated in all phases of the system development life cycle. The suite is built around the following Dell products:

1. ChangeAuditor
2. InTrust
3. Enterprise Reporter
4. Dell Knowledge Portal

Audit, Alert and Report with ChangeAuditor

Dell ChangeAuditor helps IT staff, security and compliance officers' audit, alert and report on user and administrator activity, configuration and application changes in real-time across the Microsoft-centered enterprise. This solution is critical to addressing and preventing risk of system downtime, misuse of sensitive data, failed audits and security breaches whilst ensuring business management can prove to auditors and internal stakeholders that compliance and security policies are enforced throughout the organization.

Knowing who accessed, deleted, moved, created or modified data and settings is critical to achieving internal and external compliance. Unlike native tools, ChangeAuditor provides visibility into enterprise-wide activities from one central console. Organizations can instantly see who, what, when, where, from what workstation and why a change was made, with before and after values.

What separates ChangeAuditor from other solutions is the ability to close potential security gaps by enabling customers to see the full context of how data is being handled in relation to other events and answers tough questions such as:

- How do you know if the change is suspicious?
- What other change occurred around this event and if it is critical?
- Should the user/administrator be accessing this resource?
- Does this resource contain sensitive data?
- Need to know more about the user making these changes?
- Need to know more about the user being changed?

This helps speed resolution of security issues, as well as identify misconfigurations; enabling a better understanding and forensic analysis of events and trends. If a critical change is made, an alert is sent to any device with the option to immediately respond to any threats. ChangeAuditor also provides powerful preventative controls for Active Directory, Exchange, and Windows File Server that protect objects within these environments against attempted changes deemed too dangerous to permit. Thus, attempted changes to critical files (e.g. financial data) on a file server, even with native Windows administrator privileges, not only get noticed, but are blocked at the source.

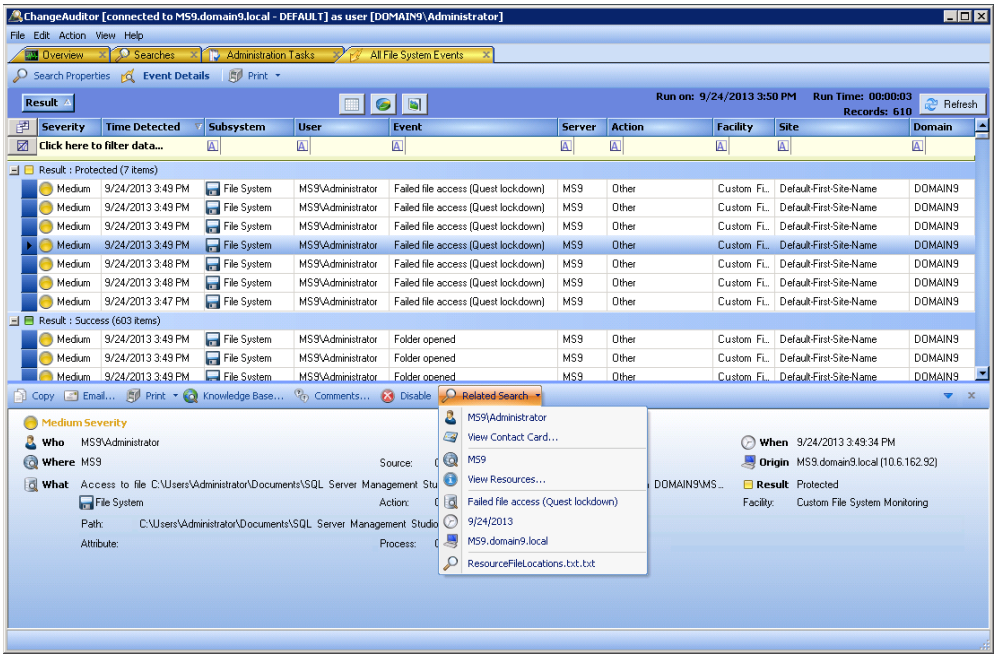

Figure 1. Prevent sensitive files from being modified or deleted with object protection and see all related searches with one click.

ChangeAuditor also simplifies external compliance audits and strengthens internal controls with over 700 out of the box auditor-ready and scheduled reports. Additionally, ChangeAuditor has

role-based access, enabling auditors to have access to only the information they need to quickly perform their job, freeing administrators to go about their daily work without interruption.

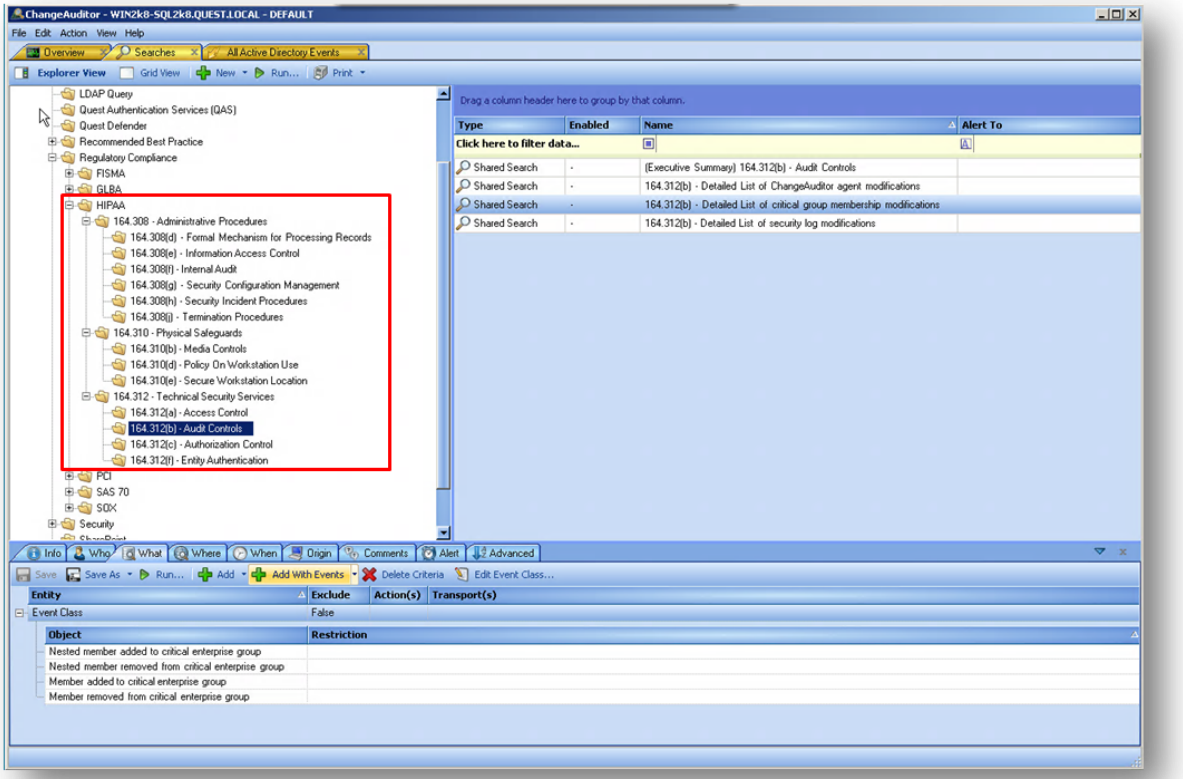

Figure 2. Built-in regulatory compliance and best practice reporting

Last but not least, ChangeAuditor has a high performance auditing engine that doesn't require native auditing to be enabled and can perform at much faster speeds for the end user than other solutions that rely on native auditing. This saves on server resources that would otherwise impact storage, processors and memory.

Forensic Investigation and Event Archival with InTrust

Dell InTrust helps organizations address regulatory compliance and internal security risks through the secure, real-time collection and compression of event logs. Using InTrust, administrators can reduce the complexity of event log management across a heterogeneous network, reduce storage administration costs and improve the efficiency of security, operational and compliance reporting. Specifically, Dell InTrust:

- Monitors user access to critical systems and applications, and enables forensic analysis of user and system activity based on historical event data
- Collects events on user and administrator activity from diverse and widely dispersed systems and applications, and presents them in an easy-to-use and complete form suitable for ongoing reporting and ad-hoc analysis
- Provides unparalleled long-term data compression at a 1:40 ratio to meet compliance requirements versus storing the same amount of data in a database, providing storage savings

- Creates a cached location on each remote server where logs can be duplicated as they are created, preventing a rouge user or administrator from tampering with audit log evidence
- Conducts an interactive search through historical event log data for on-the-spot investigation of security incidents and policy violations, and preparation of evidence for submission to the court
- Enriches SIEM with intelligent data feeds that capture crucial aspects of user activity on Windows systems, which can detect internal threats in less time and with less overhead
- Audits the use of shared and super user accounts to meet compliance-driven requirements and implement accountability of the shared accounts usage. This minimizes security risks by knowing what was done during privileged or sensitive access

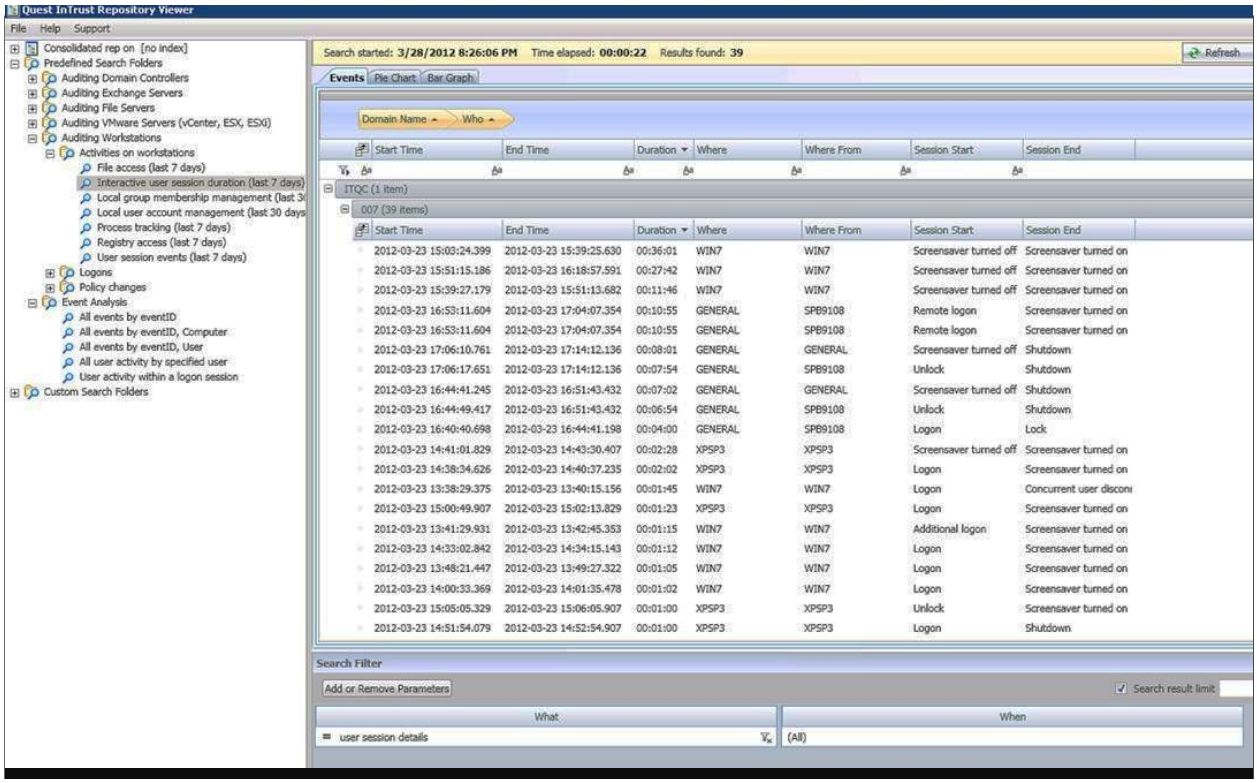

Figure 3. Event log management for security and compliance.

From Windows, to UNIX and Linux, InTrust enables you to eliminate the silos of gathering, analyzing and reporting on suspicious event data from disparate IT environments. From the time users log on until the time they log off, Dell InTrust provides a complete and connected view of the security events happening in organizations' environments. Having all this tamper-proof information easily available on-the-fly helps users address internal security policies and achieves regulatory compliance.

Assess Compliance and Security with Enterprise Reporter

Dell Enterprise Reporter collects, stores, and reports on network security and share and folder-level permissions-related information, offering a scalable solution that enables administrators to easily assess who has access to what resources, and delivers reports to consumers across the organization. These reports give you the information you need to control access to the corporate network and its data. Armed with this information, organizations can meet compliance requirements and security best practices with answers to questions auditors ask including:

- Who can do what and where?
- Who has administrative access to Windows servers and workstations?
- Who has access to what printers, shares, folders, files and SQL databases?
- How servers are configured such as general computer information, network settings, services running, installed programs and custom registry keys?
- How does the configuration of servers change over time?
- What local users and groups along with membership exist on every server?
- What software is installed on each server?
- What logins exist on each SQL Server database?

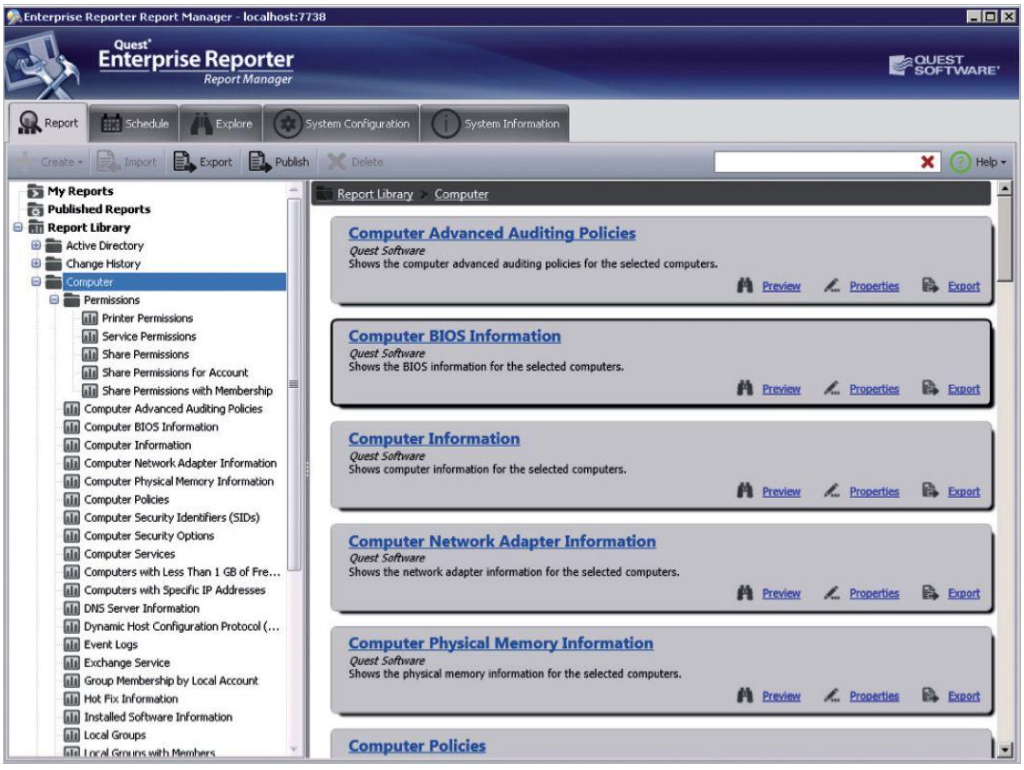

Figure 4. Enterprise Reporter provides unparalleled visibility into the configuration of critical IT assets.

Organizations can easily determine who has access to what resources, identify users with inappropriate access, and ensure that access is provided on a "business-needs-to-know" basis to ensure successful audits.

Dell Knowledge Portal

Dell Knowledge Portal offers unified web-based compliance reporting and filtering of Dell-collected monitoring and audit data for structured, audience-specific and tailored views of this information. Dell Knowledge Portal can provide supporting evidence that security policies and operational procedures for managing vendor defaults, monitoring access to network resources & protected data and other security parameters are in use. Users get access to only the information they need.

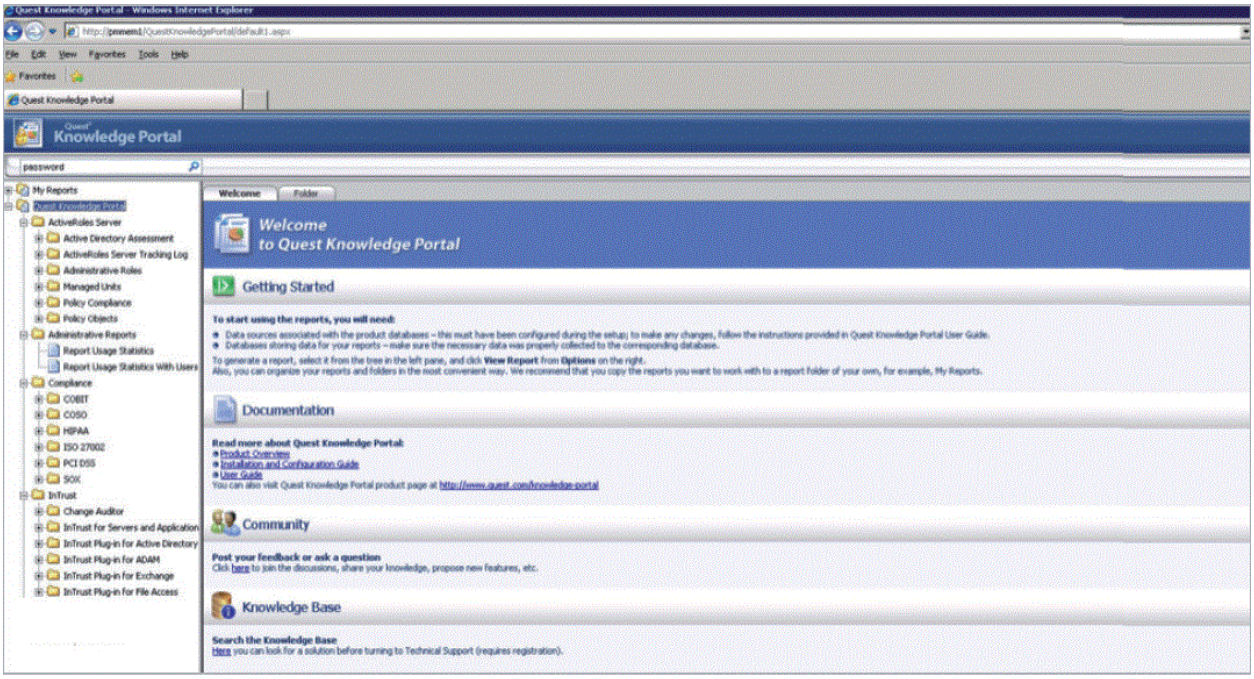

Figure 5: Consolidate data into a single pane of glass for reporting across Dell compliance solutions.

Part 3: Dell Product to Mandate Mapping Tables

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
2.1 (v3.0) 2.1 (v2.0)	Always change vendor-supplied defaults *and remove or disable unnecessary default accounts* before installing a system on the network. This applies to *ALL default* passwords, *including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals,* Simple Network Management Protocol (SNMP) community strings, etc.).	**Enterprise Reporter** provides authorized personnel (e.g. system administrators and auditors) the ability to report on password properties, the last date and time passwords changed, SNMP settings, etc.
2.2 (v3.0) 2.2 (v2.0)	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.	Once an approved system component configuration is achieved, **InTrust** can be configured to send alerts when the configuration has been changed.
2.2.1 (v3.0) 2.2.1 (v2.0)	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. **Note:** Where virtualization technologies are in use, implement only one primary function per virtual system component.	**Enterprise Reporter** can help identify the primary function of both physical and virtual servers by revealing their server type and installed software.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
2.2.2 (v3.0) 2.2.2 (v2.0)	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Each product in the **Dell GRC Product Suite** provides a variety of reports that can assist system administrators and auditors review the types of services and protocols running in a Windows environment. **InTrust** extends this functionality to heterogeneous (mixed) environments.
2.2.3 *(v3.0)* 2.2.2 (v2.0)	Implement *additional* security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	
2.2.4 (v3.0) 2.2.3 (v2.0)	Configure system security parameters to prevent misuse.	**Enterprise Reporter** can report the system security options for all windows computers in an AD domain. **ChangeAuditor** canprevent unauthorized changes from happening and **InTrust** has response actions, which can be configured to reset changes deemed to be unauthorized.
2.2.5 (v3.0) 2.2.4 (v2.0)	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and unnecessary web servers.	By identifying the installed software the cardholder data environment (CDE) **Enterprise Reporter** helps systems administrators in removing all unnecessary functionality in the CDE and auditors in verifying that nothing unnecessary is present.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
2.4 (v3.0)	*Maintain an inventory of system components that are in scope for PCI DSS.*	**Enterprise Reporter** and **Dell Knowledge Portal** can provide software component details for system component inventories.
2.5 (v3.0)	*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.*	**ChangeAuditor**, **InTrust**, **Enterprise Reporter** and **Dell Knowledge Portal** provide evidence and assist in ensuring that security policies and operational procedures for managing vendor defaults and other security parameters are in use.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
Requirement 7: Restrict access to cardholder data by business need-to-know		
7.1 (v3.0) 7.1 (v2.0)	Limit access to system components and cardholder data to only those individuals whose job requires such access.	**Enterprise Reporter** provides organizations an easy means of executing PCI DSS access control testing procedures (auditing access control policies and ensuring compliance with PCI DSS Requirement #7) by providing "who has access to what" visibility independent from AD. For heterogeneous environments, **InTrust** offers reporting of root delegation and granular privilege access on Unix and Linux systems while **Enterprise Reporter** provides reports on privileged user IDs and management of user and group access to resources across the Windows enterprise. In addition, **InTrust** and **ChangeAuditor** also offer complete access and permissions history for "who granted what to whom" details on protected file, folder, share, and NTFS "cardholder data environment" components on Windows file servers.
7.1.1 (v3.0)	*Define access needs for each role, including:* *System components and data resources that each role needs to access for their job function* • *Level of privilege required for accessing resources.*	
7.1.2 (v3.0) 7.1.1 (v2.0)	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	
7.1.3 (v3.0) 7.1.2 (v2.0)	Assign access based on individual personnel's job classification and function.	
7.1.4 (v3.0) 7.1.3 (v2.0)	Require documented approval by authorized parties specifying required privileges.	
7.2 (v3.0) 7.2 (v2.0)	Establish an access control system for systems components with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. And This access control system must include the following:	
7.2.1 (v3.0) 7.2.1 (v2.0)	Coverage of all system components	
7.2.2 (v3.0) 7.2.2 (v2.0)	Assignment of privileges to individuals based on job classification and function	

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
Requirement 8: Identify and authenticate access to system components		
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:		
8.1.1 (v3.0) 8.1 (v2.0)	Assign all users a unique ID before allowing them to access system components or cardholder data	**Enterprise Reporter** can facilitate the process of ensuring that each user account in Active Directory with access to CDE system components and cardholder data is tied to a single named person. **ChangeAuditor** can be used to review the change history of each account and continuously audit all changes to the attributes identified in this baseline.
8.1.2 (v3.0) 8.5.1 (v2.0)	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**ChangeAuditor** and **InTrust** track creation, deletion and modification of general user accounts, privileged user accounts, permission changes and other identifier objects (user attributes, group memberships, etc.) both in AD and locally on managed computers. **ChangeAuditor** supports object locking to protect against unwanted changes to user objects within AD. In addition, **Enterprise Reporter** and **ChangeAuditor** can be used to perform periodic reviews of user access to validate that access has been granted in accordance with a corresponding authorization form.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
8.1.3 (v3.0) 8.5.4 (v2.0)	Immediately revoke access for any terminated users.	The definitive record of terminated employees and contractors is stored within the HR database. This often requires an additional step of revoking of access within AD. **Enterprise Reporter** can assist with reviewing substantive access revocation samples (e.g. for the last 6 months) of terminated users. Also, **Enterprise Reporter** can report on users that have not logged in within a period of time such as 180 days. Matching user termination requests (sent from HR to authorized AD administrators) with historical disabled user account reports from **Enterprise Reporter** provides evidence that this control has or has not been in place.
8.1.4 (v3.0) 8.5.5 (v2.0)	Remove/disable inactive user accounts at least every 90 days.	Each product in the **Dell GRC Product Suite** provides a variety of reports that can assist system administrators and auditors review AD and local logons for Windows-based systems and detect user accounts that have not logged on for more than 90 days. For example, **Enterprise Reporter** can report on users that have been inactive for 90 days.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
8.1.5 (v3.0) 8.5.6 (v2.0)	*Manage IDs* used by vendors *to access, support, or maintain system components* via remote access *as follows*: • Enabled only during the time period needed *and disabled when not in use*. • Monitored when in use.	**Enterprise Reporter** can pinpoint users that were assigned remote access rights. **InTrust** and **ChangeAuditor** can report on all remote interactive logons. **InTrust** and **ChangeAuditor** can report on logons during no-business hours. **ChangeAuditor** and **InTrust** can track specific user access (i.e. all vendor accounts) and allow administrators to create reports specific to vendor ID user activity.
8.1.6 (v3.0) 8.5.13 (v2.0)	Limit repeated access attempts by locking out the user ID after not more than six attempts.	**InTrust** provides real-time alerting for successful and failed access attempts to guess a password before the account gets locked out. **Enterprise Reporter** can assist with reviewing a substantive sample of system configuration settings to verify (in each AD domain and on each computer): • authentication parameters are set to require user accounts be locked out after more than six invalid logon attempts. • password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. • system/session idle time out features have been set to 15 minutes or less In addition, **InTrust** and **ChangeAuditor** can assist organizations in continuously monitoring forced logoff & lockout policy parameters by tracking changes &
8.1.7 (v3.0) 8.5.14 (v2.0)	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	
8.1.8 (v3.0) 8.5.15 (v2.0)	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	

		attempted changes and notifying administrators of the event.
PCI DSS Section*	**Requirement**	**How Dell's GRC Product Suite Helps**
8.2 (v3.0) 8.2 (v2.0)	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.	**Enterprise Reporter** permits authorized system administrators and auditors the ability to review security options for each AD domain and computer in a cardholder data environment, including whether encryption is supported in network protocols and related system cryptography security options on local and remote machines.
8.2.1 (v3.0) 8.4 (v2.0)	Using strong cryptography, render all *authentication credentials (such as* passwords/*phrases)* unreadable during transmission and storage on all system components.	

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
8.2.3 (v3.0) 8.5.10 (v2.0) 8.5.11 (v2.0)	*Passwords/phrases must meet the following:* • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. *Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.*	**Enterprise Reporter** can assist with reviewing password policy parameter settings within a variety of CDE password configuration settings (in AD, SQL Server and locally managed Windows Servers) to verify (in each AD domain and on each computer) that user password parameters are set to require: • a minimum password length of at least seven characters • both numeric and alphabetic characters • users change passwords at least every 90 days • new passwords cannot be the same as the four previously used passwords • first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use In addition, **InTrust** and **ChangeAuditor** can assist organizations in continuously monitoring these parameters by tracking changes & attempted changes and notifying administrators of the event.
8.2.4 (v3.0) 8.5.9 (v2.0)	Change user passwords/*passphrases* at least every 90 days.	
8.2.5 (v3.0) 8.5.12 (v2.0)	Do not allow an individual to submit a new password/*phrase* that is the same as any of the last four passwords/*phrases* he or she has used.	
8.2.6 (v3.0) 8.5.3 (v2.0)	Set passwords/*phrases* for first-time use and *upon* reset to a unique value for each user, and change immediately after the first use.	
8.3 (v3.0) 8.3 (v2.0)	Incorporate two-factor authentication for remote network access originating from outside the network *by personnel (including users and* administrators) and *all* third parties, *(including vendor access for support or maintenance)*.	**Enterprise Reporter** can report on user accounts that are leveraging smart cards to assist with the process of verifying two-factor authentication. **InTrust** and **ChangeAuditor** can identify remote interactive logons for easy correlation with personnel (e.g. employee) and vendor accounts.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
8.5 (v3.0) 8.5.8 (v2.0)	Do not use group, shared, or generic *IDs*, passwords, or other authentication methods *as follows:* • *Generic user IDs are disabled or removed.* • *Shared user IDs do not exist for system administration and other critical functions.* • *Shared and generic user IDs are not used to administer any system components.*	**Enterprise Reporter** can check for existence of generic user IDs in AD domain and locally on computers. **ChangeAuditor** and **InTrust** can detect when group, shared or generic accounts are used to make changes.
8.6 (v3.0)	*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.*	**Enterprise Reporter** can report on user accounts that are leveraging smart cards to assist with the process of verifying that the authentication mechanism is assigned to an individual account and not shared among multiple accounts.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
8.7 (v3.0) 8.5.16 (v2.0)	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).*	**ChangeAuditor** can detect user access and configuration changes in SQL. **InTrust** does the same for Oracle databases. In cases where an Exchange database contains cardholder data, **ChangeAuditor** can detect instances where access that is authenticated at the application layer is being abused or circumvented such as can happen with non-owner mailbox access by another Exchange user or Exchange administrator. To the extent cardholder data exists on file servers, **InTrust** and **ChangeAuditor** also provide similar detective controls at the file access level.
Requirement 10: Track and monitor all access to network resources and cardholder data		
10.1 (v3.0) 10.1 (v2.0)	*Implement audit trails to link* all access to system components to each individual user.	**ChangeAuditor** provides evidence of CDE access to individual users by tracking administrative privileges for users managed in AD. When combined with **Enterprise Reporter**, **ChangeAuditor** links user access to specific files, folders, and shares across the Windows enterprise. **InTrust Knowledge Packs** extend visibility of CDE access to individual users outside Windows environments by tracking privilege access management (e.g. root delegation) for Unix and Linux users regardless of whether they are also managed within AD. The **InTrust** and **ChangeAuditor** families of activity logging solutions enable organizations to forensically analyze user activity on many different system components whether it is from a general user or administrator. Changes can be tracked and point to a specific user.
PCI DSS	**Requirement**	**How Dell's GRC Product Suite Helps**

Section*		
10.2 (v3.0) 10.2 (v2.0)	**Implement automated audit trails for all system components to reconstruct the following events:**	
10.2.1 (v3.0) 10.2.1 (v2.0)	All individual user accesses to cardholder data	**InTrust** and **ChangeAuditor** can track and report on individual user access to the cardholder data stored on Windows servers, Unix and Linux systems, databases and applications.
10.2.2 (v3.0) 10.2.2 (v2.0)	All actions taken by any individual with root or administrative privileges	The **InTrust** and **ChangeAuditor** families of activity logging solutions can track, report and alert on user activity with elevated user privileges on many different system components throughout the organization.
10.2.3 (v3.0) 10.2.3 (v2.0)	Access to all audit trails	**InTrust** is an enterprise audit log solution that enables organizations to connect, collect, store independently and report on auto-generated audit information across the enterprise including all attempts to access event log data. **ChangeAuditor** and **InTrust** audit and collect activity that may be associated with log tampering such as "Event Log Cleared" and "Event Log Rolled Over" events to a central database for forensic review and reporting. **Enterprise Reporter** provides visibility into permissions to native audit trail data from across the enterprise in a user friendly format. **Dell Knowledge Portal** offers unified web-based compliance reporting and filtering of this data for even more tailored views of this information. Simple searches and prebuilt reports are provided out of the box in all four audit trail monitoring solutions to preserve the security of all audit trails.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
10.2.4 (v3.0) 10.2.4 (v2.0)	Invalid logical access attempts	Both **ChangeAuditor** and **InTrust** provide failed authentication and other access attempt reporting and alerting on many different system components. This information includes the source machine, username, reason for failure and date/time.
10.2.5 (v3.0) 10.2.5 (v2.0)	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*	Both **ChangeAuditor** and **InTrust** can audit and report on the type of authentication mechanisms used to access cardholder data.
10.2.6 (v3.0) 10.2.6 (v2.0)	Initialization*, stopping, or pausing* of the audit logs.	Both **InTrust** and **ChangeAuditor** are self-auditing (i.e. have their own audit logs recording events that are separate from events captured from other sources), so any changes or attempted changes to the audit policy parameters within CDE components being monitored are tracked separate from those components (i.e. within the Dell products themselves).
10.2.7 (v3.0) 10.2.7 (v2.0)	Creation and deletion of system-level objects.	Both **ChangeAuditor** and **InTrust** provide the ability to report and alert on all system-level activity such as installation of software, modification of system registry and changes to the configuration files.
10.3 (v3.0) 10.3 (v2.0)	**Record at least the following audit trail entries for all system components for each event:**	

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
10.3.1 (v3.0) 10.3.1 (v2.0)	User identification	By enhancing the native logging capabilities of the OS and of Active Directory, both **ChangeAuditor** and **InTrust** are able to determine and secure the recording of the caller account, user ID, or AD user account attributes for each and every action in the network.
10.3.2 (v3.0) 10.3.2 (v2.0)	Type of event	Both **ChangeAuditor** and **InTrust** enhance the native logging capabilities of the OS by normalizing event information and determining what type of event occurred through either the category or ID.
10.3.3 (v3.0) 10.3.3 (v2.0)	Date and time	Both **ChangeAuditor** and **InTrust** capture the date and time of each event as it was created.
10.3.4 (v3.0) 10.3.4 (v2.0)	Success or failure indication	**ChangeAuditor** and **InTrust** both have the ability to determine the difference between successful and failed access or change attempts of many different system components including file access, authentication, and object changes.
10.3.5 (v3.0) 10.3.5 (v2.0)	Origination of event	**ChangeAuditor** and **InTrust** are always able to determine the origination of event whether that be computer/server name or an IP address.
10.3.6 (v3.0) 10.3.6 (v2.0)	Identity or name of affected data, system component, or resource	Both **ChangeAuditor** and **InTrust** provide a complete view into the audit trail of changes to many different system components including who made the change, when, where and what was affected.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
10.4 (v3.0) 10.4 (v2.0)	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	**Enterprise Reporter** provides a report that identifies domain controllers with clocks out of sync.
10.5 (v3.0) 10.5 (v2.0)	Secure audit trails so they cannot be altered.	**InTrust** provides an agent-side caching feature that protects the audit logs from modification while also removing the chance for lost logs. As the information is transferred across the Wide Area Network (WAN), the data is encrypted using 3DES 168-bit encryption. **ChangeAuditor** captures the events and communicates them back to the central database – removing from the systems and preventing any modification.
10.5.1 (v3.0) 10.5.1 (v2.0)	Limit viewing of audit trails to those with a job-related need.	**InTrust** and **ChangeAuditor** provide reporting through an access-based web portal, meaning that users can be given access to only the information they need. **ChangeAuditor** has role-based access controls that limit viewing of audit trails to only those who have specifically been assigned rights by an authorized administrator.
10.5.2 (v3.0) 10.5.2 (v2.0)	Protect audit trail files from unauthorized modifications.	**InTrust** offers two storage methods, NAS and Windows File Servers. EMC Centera provides data protection through proprietary methods. The information held within the repository is in a proprietary format and can be locked down through native methods. Both **ChangeAuditor** and **InTrust** also have lockdown options for audit trails stored on Windows servers. In addition, these products self-audit so that all

		configuration changes made within the tools themselves are tracked and audited as well.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
10.5.3 (v3.0) 10.5.3 (v2.0)	Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.	**InTrust** provides a full consolidation solution which enables organizations to take audit log data from locations from around the globe and consolidate this information in a single location. Similarly, **ChangeAuditor** captures events in real time and sends them to its central database server immediately. These audit trails are separate from the audit sources and can be made secure even if those systems become compromised.
10.5.4 (v3.0) 10.5.4 (v2.0)	Write logs for external-facing technologies onto a *secure, centralized,* internal log server *or media device*.	**InTrust** can securely collect logs from external facing technologies (firewalls, gateways, etc.) and report on all syslog data being created at the network layer. **ChangeAuditor** has an additional facility to write events to the event log (at the same time securely storing the events in its central DB) for other tools and services to consume (e.g. **InTrust** and other log collection tools).
10.5.5 (v3.0) 10.5.5 (v2.0)	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)	**InTrust** provides real-time alerting for successful and failed access attempts to critical areas. This includes the long-term storage area of audit log information. **InTrust** and **Change Auditor** can also be used to monitor the integrity of audit log files that reside on Windows servers.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
10.6 (v3.0) 10.6 (v2.0)	Review logs *and security events* for all system components *to identify anomalies or suspicious activity*. Note: Log harvesting, parsing, and alerting tools may be used to meet *this Requirement*.	**InTrust** can monitor and alert on patterns of unusual activity such as multiple failed logon attempts, logons during non-business hours and other sequences of events configurable by the user. **InTrust** reports can be generated on a daily basis and distributed to necessary persons. **InTrust** provides interactive tools for ad hoc log analysis that quickly search throughout the consolidated event log data and help easily interpret results as they are shown in a normalized format **ChangeAuditor** provides customizable dashboards with the most up to date events (focused on each technology, geo or function: All Exchange Events, File System activity in the last 24 hours, SharePoint file check out in EMEA, etc)
10.6.1 (v3.0)	*Review the following at least daily:* • *All security events* • *Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD* • *Logs of all critical system components* • *Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).*	
10.6.2 (v3.0)	*Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.*	
10.6.3 (v3.0)	*Follow up exceptions and anomalies identified during the review process.*	Both **InTrust** and **ChangeAuditor** provide exception based alerting that assist during the review process.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
10.7 (v3.0) 10.7 (v2.0)	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).	With a 40:1 compression ratio, **InTrust** provides a long-term storage (one to seven years) area at a greatly reduced cost. **ChangeAuditor** provides central storage based on Microsoft SQL and is limited only by the size of disk where the DB exists.
10.8 (v3.0)	*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.*	The documented consistent use of automated security monitoring tools like **ChangeAuditor** & **InTrust**, or the documented and proactive use of **Enterprise Reporter** & **Dell Knowledge Portal** can provide supporting evidence that security policies and operational procedures for monitoring access to network resources and cardholder data are in use.
Requirement 11: Regularly test security systems and processes.		
11.5 (v3.0) 11.5 (v2.0)	Deploy *a change-detection mechanism (for example,* file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Both **InTrust** and **ChangeAuditor** can be used to monitor changes to Windows and NetApp/EMC file systems and otherwise monitored files of all types on many different system components. **Enterprise Reporter** can report on system settings and file-based attributes to determine if any files have been altered.
11.6 (v3.0)	*Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.*	The documented consistent use of automated security monitoring tools like **ChangeAuditor** & **InTrust**, or the documented and proactive use of **Enterprise Reporter** & **Dell Knowledge Portal** can provide supporting evidence that security policies and operational procedures for security monitoring are in use.

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
Requirement 12: Maintain a policy that addresses information security for all personnel.		
12.3.4 (v3.0) 12.3.4 (v2.0)	*A method to accurately and readily* determine owner, contact information, and purpose *(for example,* labeling, *coding, and/or inventorying* of devices)	**InTrust**, **ChangeAuditor**, and **Enterprise Reporter** enhance the ability of native operating system services and logs to correlate device information (IP addresses, hostnames) to their respective owners.
12.10.5 (v3.0) 12.9.5 (v2.0)	Include alerts from *security monitoring systems, including but not limited to* intrusion-detection, intrusion-prevention, *firewalls*, and file-integrity monitoring systems.	**InTrust** and **ChangeAuditor** are designed to capture and generate alerts on user access to provide additional context to SIEM solutions. These Dell GRC tools substantially enhance an organization's security monitoring function and thereby support its incident response processes by providing information security alerts.
Appendix A, Requirement A.1: Shared hosting providers must protect the cardholder data environment		
A.1.3 (v3.0) A.1.3 (v2.0)	Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	**Enterprise Reporter** and **InTrust** can be used by a hosting service provider to help ensure logging and audit trails are enabled and unique to each entity's cardholder data environment. For example, **InTrust's** log indexing, search capability and repository data segregation options all assist in distinguishing among various entities being monitored. In addition, **ChangeAuditor** organizes events into objective categories so that data can be easily grouped/sorted and filtered to provide unique CDE views of data (i.e. segmented based on entity).

PCI DSS Section*	Requirement	How Dell's GRC Product Suite Helps
A.1.4 (v3.0) A.1.4 (v2.0)	Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	**InTrust** can be leveraged by a hosting service provider to assist technical personnel with timely forensic investigation processes in the event of a compromise. **ChangeAuditor** also enables forensic reviews by organizing events into intuitive categories (Who, What, Where, etc) so that data is easily grouped/sorted and filtered to provide segmented views of data based on entity relationships and event meta data correlation.

*Except for the 12 high level requirements where the language of PCI DSS version 3.0 (v3.0) is used, this chart contains applicable PCI DSS requirements from both DSS v2.0 & v3.0. The language in the detailed requirements that is new with the release of v3.0 is italicized.

Conclusion

With the proliferation of information security threats mixed with the complexity of compliance mandates, organizations today need as much compliance automation they can get. The Dell GRC Product Suite helps organizations automate many of the assurance safeguards required by today's IT security mandates while also providing foundational IT security measures. While not a replacement for network vulnerability tools, when regularly used as part of a continuous monitoring program, InTrust, ChangeAuditor, and Enterprise Reporter can discover a host of information system vulnerabilities (e.g. outdated patch levels, unauthorized ports, protocols, and services) before network vulnerability scanning tools and technical surveillance countermeasure surveys can discover them. By enabling the assurance functions of real-time audits, continuous monitoring and the generation of information system documentation for discrete environments, the Dell GRC Product Suite helps organizations not only watch their production operating environments but monitor critical controls in security architectures that are anticipated in all phases of the system development life cycle. For more information, visit http://software.dell.com/solutions/compliance-and-it-governance/

About the Authors

Steven Marco, President has a passion for IS Security and over 18 years as a leader in executing various regulatory compliance mandates and Health IT. A CISA since 1999, he helped pioneer Internet Security Services and manage risk for numerous Fortune 500 companies while at Deloitte

& Touche. At Resources Global Professionals, he led IT through their Sarbanes Oxley 404 audit and successful IPO in 2002. He successfully pioneered a Health IT professional services line leading hundreds of compliance and security projects. Prior to founding Modern Compliance Solutions, Steve was Product Director at DirectPointe, where he successfully integrated HIPAA and PCI security protocols for their Healthcare and MAS clients. Steve holds a Bachelor's Degree from Ryerson University in Computer Information Systems Management and Corporate Law. For more information, visit http://moderncompliancesolutions.com/

Joe Grettenberger, CISA, CCEP has over 25 years experience as an IT Assurance professional with 8 years of technology auditing experience both in the public and private sectors. Having started his own consulting practice in 2008, Grettenberger is certified as an information systems auditor (CISA) and compliance & ethics professional (CCEP). He has served clients for over 5 years as an IT governance and risk management consultant covering a wide range of IT assurance issues within the regulatory, legal, and industry compliance space. Grettenberger has held assurance and advisory positions at a number of organizations including Quest Software, Vintela, Center 7, Franklin Covey and SAIC. He was a recent participant in the Internet Security Alliance initiative to promote cross-industry IT security standards and has also participated in several other standard-setting best practice initiatives such as serving on the SunTone Architecture Council and chairing the MSP Association's Best Practice Committee. For more information, visit http://moderncompliancesolutions.com/

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.software.dell.com