Abstract
This white paper explains how the Configuration Compliance solution can enable companies to ensure visibility of the IT infrastructure, automate remediation and increase efficiency. The document will show the benefits of integrating IT infrastructure management technologies such as Network Configuration Manager, Storage Configuration Advisor and vCenter Configuration Manager into the RSA Archer platform.

June 2012
Table of Contents

Executive summary .................................................................................................................. 4
Audience ................................................................................................................................. 4
Introduction .................................................................................................................................. 5
  Infrastructure Compliance Challenges ................................................................................. 5
IT Infrastructure Configuration Management ............................................................................ 6
  EMC Storage Configuration Advisor .................................................................................. 6
  EMC Network Configuration Manager ................................................................................. 7
  VMWare vCenter Configuration Manager ............................................................................ 9
IT GRC as a Business Imperative ............................................................................................ 11
  Platform Approach to IT GRC ............................................................................................ 12
RSA Archer Integration Scenarios ............................................................................................ 13
  Scenario 1: Compliance Data Consolidation ....................................................................... 14
  Scenario 2: Detail Control Mapping ..................................................................................... 15
Recommendations .................................................................................................................... 16
  Focus on Quick Wins ........................................................................................................... 17
  Drive Automation via Integration ......................................................................................... 17
  Show the Cost Saving ............................................................................................................ 18
  Make it Easy for Executives ................................................................................................. 18
  Involve Key Stakeholders Early .......................................................................................... 18
Conclusion ............................................................................................................................... 19
Appendix .................................................................................................................................... 20
Executive summary

In today’s fast changing market, organizations must be quick to respond to changes as well as be efficient and lower costs. In addition, the journey to the cloud has been driving the IT organization toward better utilization of their infrastructure through virtualization of compute and storage, and optimization of networks. However, this transformation also leads to new challenges relating to IT visibility and compliance complexity.

What most companies need is an effective approach to governance, risk management, and compliance (GRC). IT infrastructure compliance needs to be a part of the overall GRC strategy. It’s critical to address the internal complexities brought on by today’s dynamic physical and virtual data centers with both new technologies and new ways of doing business.

GRC used to start by discrete projects with focus on policy definition, manual testing of controls and minimal use of risk management models. Over the years, companies started to incorporate IT risk management & IT governance with periodic testing of IT controls via web-based questionnaire method. Today we see the linkages between enterprise GRC, information GRC, and IT operations GRC becoming more transparent. Technologies are able to enable tighter integration for automated control monitoring and better management of risks.

EMC, RSA and VMware are committed to expanding the benefits companies are receiving from RSA Archer and infrastructure management software investments. The EMC Configuration Compliance Solution provides a seamless integration of RSA Archer with:

- EMC Storage Configuration Advisor (SCA)
- EMC Network Configuration Manager (NCM)
- VMware vCenter Configuration Manager (vCM)

Most organizations are asking for help from technology vendors on addressing the cost of compliance and increasing system uptime. In many scenarios, automation is the key to their success.

Audience

This white paper is intended for Infrastructure Administrators, Storage Administrators, Network Administrators, RSA Archer Administrators, Information Security Architects or Compliance Officers.
**Introduction**

EMC is leading the industry in enabling companies of all sizes to progress along their journey to the cloud. This journey can be divided into 3 phases:

1. **Phase 1** – Focus on hardware consolidation and virtualization of non-mission critical IT production apps.
2. **Phase 2** – Assess potential benefits from virtualizing mission critical apps.
3. **Phase 3** – Explore new opportunities to drastically enhance the speed and agility of IT

This transition, together with competitive, internal and regulatory pressure, has created many new challenges.

**Infrastructure Compliance Challenges**

The problems that both IT and Information Security teams facing are in 3 areas:

- **Lack of IT Visibility**
  - $26.5B revenue lost in 2011 due to IT downtime
  - Infrastructure outage can cost average of $5,000 per minute

- **Configuration Complexity**
  - 85% of IT problems are related to organization and technology change
  - 78% of outages caused by misconfigurations due to changes

- **Increasing Regulatory Requirements**
  - Only 1 in 10 companies can effectively measure infrastructure compliance

First, many organizations may not have deep visibility into the IT infrastructure from the security and compliance standpoint. Information is tracked via manual processes and there are days or weeks of delay. There is no integrated approach to provide more
visibility to high level executives or blend the information from IT infrastructure into the overall compliance context.

Second, security teams often do not realize there are better ways to collect information and assess risk in the organization. In many instances, it’s possible to leverage EMC and VMware technologies to collect IT data from the sources automatically and perform correlation, analysis, and assessment.

Third, companies spend a significant amount of time proving compliance to internal and external auditors. Without automation, manual data collection can be very unreliable.

**IT Infrastructure Configuration Management**

Many tools out there may provide IT a partial picture of the infrastructure such as the changes to server environment but not the changes to network and storage environment. Others may cover all infrastructure domains but do not provide prebuilt templates, change management or remediation capabilities.

This inconsistent vision of the entire infrastructure makes compliance management and reporting a very challenging part of GRC operations. By offering complete coverage across domains, companies will have a complete vision of the state of IT infrastructure. EMC, RSA and VMware can provide the coverage across the entire infrastructure, providing organizations the visibility to make compliance management an efficient, cost effective and low risk process.

There is a big advantage of using EMC and VMware technologies to integrate into existing RSA Archer framework and enhance the values. It’s critical to have an understanding of the capabilities of infrastructure management tools.

**EMC Storage Configuration Advisor**

EMC Storage Configuration Advisor tracks and reports changes to storage resources and ensures that they are compliant with defined storage configuration policies. Some examples of storage policies are:

- Internal configuration policies
- Industry best practices
- EMC E-lab interoperability
- Multipath management

Table 1 in Appendix provides more examples of how organizations can utilize this technology for PCI DSS 2.0 compliance effort.

Storage Configuration Advisor leverages agentless discovery, near-real-time change tracking, and configuration policy validation to identify issues before they can impact service levels. It also provides change history and service analytics to help IT improve processes and resource planning. Finally the technology provides recommendations across storage infrastructure.
EMC delivers Storage Configuration Advisor on hardware or virtual appliance that includes the application and its data repositories. It uses a web-based user interface and employs industry-standard agentless discovery based on VMware API, WMI, SSH, SNMP, and SMI-S standards. The below diagram explains Storage Configuration Advisor’s architecture.

The key benefits of Storage Configuration Advisor are:

- **Efficient Change Monitoring and Validation**
  - Validate host and infrastructure interoperability against defined policies
  - Automatically document configuration changes and violations

- **Lower Risk of Changes**
  - Roll out infrastructure upgrades with continuous configuration validation
  - Improve MTTR by rapidly identifying changes that impact service levels

- **Operational Planning and Oversight**
  - Understand current trends and their impact on change and configuration management processes
  - Automate documentation enabling audit readiness

**EMC Network Configuration Manager**

EMC Network Configuration Manager helps organization keep network components compliant in a number of ways. Some use cases are:
• Design, enforce and report on adherence to complex network policies. The policy enforcement could be for the entire domain or just one network site or subnet

• Leverage best-practice templates to schedule and deploy any-scale change quickly through distributed architecture and workflow capabilities

• Demonstrate on demand compliance and its change/control process

• Report on historical compliance of the managed infrastructure using the configuration and policies in place on the date selected

Network Configuration Manager has an intuitive graphical network view and automates complex and routine engineering tasks, such as adding devices and connections, with drag-and-drop simplicity.

One important capability of Network Configuration Manager is its real-time auto discovery of network devices and logical and physical topology information. Being able to collect network asset information and track against enterprise compliance policies is a critical component of GRC operations.

Another advantage of using Network Configuration Manager is that it allows the view of configuration data, in a vendor-neutral format, using device modeling and merges configuration data and device variables with best-practice templates to help ensure compliance. This capability is delivered via the powerful Automation Library.
These templates are key parts of IT GRC process to make sure the network is compliant with industry regulation such as PCI DSS 2.0 (See Table 2 in Appendix).

The key benefits of Network Configuration Manager are:

- **Control Network Change**
  - One system to manage a multivendor network and ensure compliance across its entire lifecycle

- **Increase Operating Efficiency**
  - Lower costs and simplify operations; increase network and service availability; and deliver services and respond to business needs faster

- **Ensure Network Compliance**
  - Detect compliance states, flag violations and fix problems to reduce business risk

**VMware vCenter Configuration Manager**

VMware vCenter Configuration Manager is a policy-driven configuration automation solution that detects deep virtual and physical changes and checks whether those changes are compliant to industry, regulatory or internal self-defined best practices. It helps organizations avoid configuration drift by remediating systems to bring them back into compliance. Some examples of use cases are:

- Managing change
- Controlling risk
- Automating operating system, software provisioning and patching with vSphere integration

vCenter Configuration Manager automates critical IT configuration management and compliance processes across thousands of assets, security and configuration settings from vSphere, VMware ESXi™ and ESX®, Windows, UNIX or Linux servers and user desktops.

Table 3 in Appendix provides a full list of how organizations can use vCenter Configuration Manager for PCI DSS 2.0.

This technology is “cloud ready” as it allows IT organizations to detect changes quickly and manage host compliance across multiple VMware vCloud Director’s instances and guests.

The advantage of using vCenter Configuration Manager is its rule building capability. The Rule Wizard will help IT organizations meet internal and external standards.
The key benefits of VMware vCenter Configuration Manager are:

- Policy Driven Configuration Management
  - Provision IT approved OS images & software packages
  - Patch to mitigate known vulnerabilities
- vSphere Compliance Checker
  - Check a small number of VMs against vSphere hardening Guidelines
- Ensuring Compliance for Hybrid Cloud Workloads
  - Ability to manage guest level compliance across Clouds
  - Certified deployment models for vCloud Service Provider Partners

**IT GRC as a Business Imperative**

The emergence of IT GRC as a strategy for protecting the enterprise from IT risk while removing barriers to growth is the result of a number of factors:

1. Demands on corporate governance
2. Multi-faceted risk environment
3. Growing regulatory requirements
4. Disappearing boundaries in the hyper-extended enterprise

These elements require stronger collaboration between IT and Information Security. Today, there is a need to have the transformation to a more programmatic approach with the use of technology.
Platform Approach to IT GRC

Organizations frequently rely on a document-centric, paper-based approach to risk and compliance management, rarely attending sophistication beyond electronic documents and spreadsheets. Aside from being error-prone and inefficient, this approach makes it difficult to share information, thereby reinforcing silos. RSA Archer provides a technology architecture that integrates with EMC/VMware systems to provide a cohesive view.

The integrated solution not only provides compliance data for configuration violations and vulnerabilities but also blends with:

- Risk analytics
- Loss events
- Logs
- Document and records retention data
- Accounting and HR information

All of this data is scattered across multiple tools and systems. RSA Archer aggregates the data putting risks, threats, incidents and compliance deficiencies into business context and enabling prioritization of the response based on what is most significant to the organization.

The key characteristics of RSA Archer platform include:

- **Centralized Views** – A central view of risk and compliance activities provides a single lens through which stakeholders can identify threats early and prioritize
issues, as well as improve efficiencies by applying a single process to multiple regulations.

- **Automation** – Through automation, organizations achieve continuous risk and controls monitoring as opposed to the point-in-time spot checks of the past. Technological capabilities required include advanced risk analytics and modeling, automated controls tied to business rules engines, advanced content and process management capabilities, and embedded GRC control points.

- **Integrated Systems** – Multiple point solutions that span different areas of the infrastructure are costly to manage, fail to deliver a holistic view of the enterprise and cannot correlate analysis to provide reliable conclusions. Integration enables management and reporting across the enterprise.

- **Flexibility** – The platform is adaptable in order to evolve as the business evolves. Furthermore, business is able to make changes and build out applications to solve business programs without relying on costly, time-intensive custom development.

**RSA Archer Integration Scenarios**

There are several ways to get data from the infrastructure management tools into RSA Archer. When evaluating options, organizations should look into variables such as regulation, timeframe, goals, etc. Some of the key questions are:

1. With what industry regulatory requirements must the company comply?
2. At what stage of a GRC program is the company?
3. What are the most urgent issues?
4. What are the easy targets?

The basic integration mechanism is RSA Archer’s Data Feed Manager (DFM). With EMC infrastructure management technologies, organizations can automatically and easily collect and evaluate vulnerability or configuration of Network, Storage and Compute.

EMC Network Configuration Manager, Storage Configuration Advisor and vCenter Configuration Manager have their discovery, scanning and analysis engine which is efficient for a particular infrastructure domain. Therefore it should be a better method of getting data from these automated scans for compliance assessment because they are reliable and faster than other methods.
Scenario 1: Compliance Data Consolidation

Consolidating data could be a simple use case to have all IT infrastructure information in one location. This scenario utilizes the summary reports from each of the management technologies and rolls everything into Archer’s dashboard. The overall process can be summarized in the following steps:

1. Configuration management tools are setup to perform configuration checks against preset policies within those tools.
2. Once the tests or checks are executed within those tools, the scanned results are summarized into summary reports.
3. Each report will contain basic information such as device name, pass/fail, rule, description, etc.
4. Data Feed Manager will reach out to either SQL database or .csv location and import those summary reports.
5. The feeds are setup so that data is stored in either Devices or Configuration Check Results application.
6. In some instances, there could be new On-Demand Applications (ODAs) because it depends on whether there is a need to pull additional data from the management tools.

This method gives users more power and flexibility to map IT assets and vulnerability states to defined Business Units, Regions or Criticality. For organizations that have specific needs to track a certain area of the IT infrastructure, this method can be a quick win to provide such tracking mechanisms without manual effort or education of configuration management technologies.
Scenario 2: Detail Control Mapping

This scenario requires a more comprehensive mapping exercise and building of data feeds. The benefit is that organizations can monitor specific controls which could be automatically checked by the configuration management tools.

Some examples of use cases are:

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Procedure Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Windows Server 2008 Member Server Idle Time before suspending a session</td>
<td>Windows Server 2008 Member Server Idle Time before suspending a session should not be longer than 15 minutes of inactivity. When not being used, accounts should be logged off from the system console.</td>
</tr>
</tbody>
</table>
| Network        | Disable services per specified interface | The following interface services will be checked if they are disabled, if not then they will be disabled on the specified interface.  
• ICMP redirects  
• ICMP unreachable  
• ICMP mask reply messages  
• Proxy-Arp  
• Directed Broadcasts |
| Storage        | Ensure all assets in a storage area network have latest vendor-supplied patches | Install the latest releases, updates, or patches within one month of release from the vendor. |

In a typical environment, there could be hundreds or thousands of control procedures setup to automatically scan for violations. In order to ensure integration between RSA Archer and infrastructure management technologies, the following process provides an overview of how it would work:

1. Each tool must be configured so that policies, rules or tests are configured and defined. For example, NCM must be set up with a test such as "Disable services per specified interface" in order to feed the result data of that rule into Archer.
2. Mapping content of control procedures and the results from each tool must be done within Archer's content framework prior to pulling data. This content will be mapped manually to Control Procedures.
3. Devices feed will populate the Devices application with data with information such as Device Name, IP Address, Device Type, etc.
4. Scan result feed will populate Configuration Check Results application with the compliance results from each tool.
The architecture diagram below demonstrates how different areas in Archer could be structured.

The content hierarchy starts with Authoritative Sources such as PCI, HIPAA, SOX or internal compliance requirements. Control Standards are different aspects of each source and contain multiple Control Procedures for checking compliance. Each Control Procedure will detail a specific action that must be executed and result in either Compliance or Non-Compliance.

There are two ways for testing a control procedure:

- **Manual** – A web-based questionnaire will be sent to the IT asset owner to respond.
- **Automated** – This is where the integration happens and all tests or scans occur automatically.

**Recommendations**

GRC implementation can vary based on industry regulations, immediate business needs, customer requirements or security breech events. Some organizations might already use IT GRC technology to align controls with departmental, corporate policies and regulations. However, most organizations still function as silos and do not have the right technologies or processes to measure activities, provide efficiencies, and evaluate risks.

An IT GRC platform should help an organization:

- Define IT policies and controls based on external and internal requirements
- Manage policy content
- Map policies to controls
- Evaluate IT risk
• Automate auditing and regulatory reporting

This effort will require collaboration amongst the process owners and technical owners in order to maintain compliance in the IT infrastructure. The integrated solution of RSA Archer/EMC/VMware is an example of using the right tool set for driving collaboration. In order to evaluate, the below criteria could be used for assessing each scenario:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Scenario 1 Compliance Data Consolidation</th>
<th>Scenario 2 Detail Control Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalability</td>
<td>Good</td>
<td>Average</td>
</tr>
<tr>
<td>Granularity</td>
<td>Generic</td>
<td>Detail</td>
</tr>
<tr>
<td>Complexity</td>
<td>Simple</td>
<td>Complex</td>
</tr>
<tr>
<td>Feed Frequency</td>
<td>High</td>
<td>Average</td>
</tr>
</tbody>
</table>

But, the secret to success is not just in the right platform, it’s also in the right management approach to people and processes.

Focus on Quick Wins

An approach to focus on early quick wins will make it easier for the organization to change. This is applicable to starting a new IT GRC strategy or revising an existing one. Below are some examples to start with:

• Focus on formalizing the risk process by taking some risk metrics from existing IT infrastructure management technologies.
• Provide better visibility and awareness of risk at the senior executive level
• Report on new risks which can be used to justify new security projects
• Watch for inconsistency in processes, especially when it comes to control testing
• Drive automated control testing for existing manual processes or even questionnaire
• address compliance results which could be a very costly area when the company is fined
• Bring in standardization and increase collaboration between Information Security and IT organizations

Drive Automation via Integration

IT tools such as VMware vCenter Configuration Manager (vCM), and EMC Network Configuration Manager (NCM) and Storage Configuration Advisor (SCA) help to monitor configuration settings and measure vulnerabilities in the IT infrastructure. They collect data automatically and to perform correlations, analysis, and assessments.
An advantage of using these technologies is their integration with a GRC framework such as RSA Archer. Most organizations collect infrastructure information manually either via spreadsheet, web portal, or archiving. This process can take time and is prone to being out-of-date or unreliable due to human error. Integration with a GRC framework allows these processes to happen automatically.

**Show the Cost Saving**

Cost savings can be achieved in many different ways after compliance processes are implemented. The obvious value is the improvement in an organization’s external audit posture. Cost saving can also be translated from other metrics such as:

- Percentage improvement in availability of critical business systems and processes
- Reduced number of trouble tickets
- Percentage of time IT staff needs to spend on problem management
- Reduction in time spent planning and validating compliance with configuration best practices, security policies and industry regulations
- Number of configuration violations identified
- Reduction in service impacting events caused by improper configuration
- Reduction in time spent remediating configuration violations

These metrics can also help to control company budget, avoiding over-spending or under-spending. IT GRC strategy can only work if its success is proven by improving the organization’s capability to effectively address IT risks and economically align processes.

**Make it Easy for Executives**

There is a lot of complexity behind infrastructure management technologies or IT technologies in general. However, their results can be used by executives if the reporting provides a simple way to roll up compliance data. A GRC framework such as RSA Archer allows quick creation of simple dashboards with information such as the current state of process and control compliance, vulnerabilities, and IT asset use.

Another argument for simplified compliance reporting is to meet the needs of internal and external auditors. Without automation made possible by an integrated compliance framework, it’s very likely that the data collected is inaccurate.

**Involve Key Stakeholders Early**

GRC strategies can be driven from either the top-down or bottom-up. IT GRC will have more IT-centric requirements when driven from the bottom-up. Alternatively, Enterprise GRC or eGRC will be more focused on enterprise risk and driven from top-down. Both approaches will require a certain level of coordination amongst an organization’s IT, security, audit, and risk management teams.
One key to success is to allow time to negotiate change. People need time to digest the impact of a new way of thinking or doing things and assess what it means to them and their jobs.

**Conclusion**

Understanding of key considerations and available options are critical to a successful GRC implementation. With the journey to the cloud, this transformation will also accelerate companies’ IT GRC journey. Therefore, the organization should have an understanding of in-house infrastructure technologies, their capabilities and integration options.

EMC’s infrastructure management portfolio has been helping its customers to provide complete compliance and service assurance with the below proven results:

- **80%** faster problem identification
- **60%** faster resolution
- **2X** more efficient IT operations

The values of EMC/RSA/VMware partnership provide (1) End-to-end Visibility, (2) Automated Compliance and (3) Effective Remediation:

<table>
<thead>
<tr>
<th>Values</th>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-to-end Visibility</td>
<td>• High Level Summary View Dashboard • IT Operation Dashboard • Detail Compliance Violation</td>
<td>• Summarize IT information relative to existing compliance programs • Reduce time spent preparing for audit via single reporting engine</td>
</tr>
<tr>
<td>Automated Compliance</td>
<td>• Compliance Policies &amp; Templates • Configuration Checks Automation Against Policies • Internal IT Best Practice Standards</td>
<td>• Provide compliance validation and change management • Avoid manual assessment via silo processes</td>
</tr>
<tr>
<td>Effective Remediation</td>
<td>• Contextual Launch to Specific Remediation Technology • Recommendation to Remediate</td>
<td>• Automate remediation to close compliance gaps quickly with minimal effort</td>
</tr>
</tbody>
</table>

Technology improvements not only help EMC’s customers ensure compliance but also provide them competitive advantages in the market place. That means companies can be more agile and quicker to respond to business needs while improving efficiencies and lowering costs.
## Appendix

### Table 1. PCI DSS 2.0 Applicability Matrix for EMC Storage Configuration Advisor

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Controls Addressed</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirement 2:</strong> Do not use vendor-supplied defaults for system passwords and other security parameters</td>
<td>2.2</td>
<td>SCA has rules for checking SAN configuration against industry accepted best practices and EMC Support Matrix (e.g. eLab) such as single initiator zoning, soft versus hard zoning, and default zoning.</td>
</tr>
<tr>
<td><strong>Requirement 6:</strong> Develop and maintain secure systems and applications</td>
<td>6.1, 6.2</td>
<td>SCA discovers Solutions Enabler, PowerPath, some third party MP drivers, HBA driver and firmware, switch OS and firmware, and array microcode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SCA can also check SAN storage devices against EMC Support matrix rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The integration with RSA Archer will help establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.</td>
</tr>
<tr>
<td><strong>Requirement 10:</strong> Track and monitor all access to network resources and cardholder data</td>
<td>10.3.2, 10.3.3, 10.3.6</td>
<td>SCA tracks changes to the SAN configuration in near real time. Each change logged by SCA also includes date and time. The name of the SAN asset is identified when changes happen as well.</td>
</tr>
</tbody>
</table>

### Table 2. PCI DSS 2.0 Applicability Matrix for EMC Network Configuration Manager

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Controls Addressed</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data | 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6, 1.2, 1.2.1, 1.2.2, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.8 | NCM is capable of accepting Syslog and Traps information from devices. This is to monitor the network for changes completed outside of the configuration management system.  
Network diagram can also be used to validate Layer 3 connectivity. NCM reports will also define for each connection, what technology is in place such as ATM, Frame relay, and Point-to-Point.  
User access to secured network components are constraint by access-list. A permission scheme in NCM can be defined for users to access resources and operations needed to perform their jobs.  
Since only a small amount of documentation can be stored on a firewall or router, NCM supports the creation of network and device objects which can store comments or attachments. NCM templates can also be used to define best practices and tests can be created to enforce these best practices. |
Device State Report provides total devices out of sync between startup and running configuration which could result in vulnerability.

NCM templates consist of samples for implementing a DMZ with inbound / outbound traffic to only protocols that are necessary for the cardholder data environment.

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

2.1, 2.1.1, 2.2, 2.2.2, 2.2.3, 2.2.4, 2.3

NCM has prebuilt templates for detecting default password of network devices or disabling unnecessary and insecure services and protocols. Users can define association of these templates with specific PCI requirements.

NCM allows a wide variety of communications protocols including SSH, SCP, Telnet, SNMP V1, SNMP V2c, SNMP V3, modems and terminal servers. It is recommended that whenever a device supports the secure protocols SSH, SCP and SNMP V3, they should be used. Using Secure Shell Protocol (SSH) for network device communication provides encrypted communications between the device server and devices for issuing configuration updates and polling configuration changes.

Many devices are also capable of using SNMP V3 for network management. NCM provides SNMP V3 manageability using authorization and privacy protocols. SNMP V3 in conjunction with SSH, provides the highest level of security available to manage network devices.

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

4.1

VPN Encryption template can be used to associate with cryptography and security protocols requirements to safeguard sensitive cardholder data during transmission over open, public networks.

**Requirement 6: Develop and maintain secure systems and applications**

6.1, 6.4.1, 6.4.2

NCM can be used to prepare for OS upgrades by providing OS Inventory reports, and by providing hardware reports for verifying memory prerequisites. The NCM OS Manager can be used to deploy new OS versions to many types of network devices, including some wireless access points.

For change control procedures of system components, NCM’s job description field should be used to reference change tickets and/or include full change description.

**Requirement 8: Assign a unique ID to each person with computer access**

8.3, 8.5.13, 8.5.14, 8.5.15

Users can customize TACACS Server and RADIUS Server templates in automation library to satisfy authentication requirement of remote access to the network by employees, administrators and third parties.

NCM contains four different types of authentication, each of which allows the administrator to control the number of logins which a user can attempt before the account is
With this authentication mechanism, user accounts are authenticated against an internal database in NCM, external TACACS+ server, RADIUS server or LDAP server. Administrators can set an explicit limit to the number of authentication attempts a user can have before the account is locked. The administrator should set this to less than six.

When a user session is locked out in NCM, the user account will not be unlocked until explicit action is taken by the administrator to unlock the user ID.

The default user session timeout in NCM is 30 minutes, after which the user’s session will automatically timeout and require a login to continue. This can be controlled through the JMX console, which can be accessed by the system administrator.

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

10.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4, 10.5, 10.5.1, 10.5.2, 10.6

NCM maintains an audit log of all device accesses made, as well as any device change events detected on the device via notification from the device (Syslogs, or Traps), or timed configuration pull.

For automated audit trails, NCM logs all accesses to protected resources through the user interface or API, regardless of whether the user is a system administrator or not. It exposes both AuthorizationFailedEvent and AuthorizationSucceededEvent for any logical access attempts.

Many other events related to creation and deletion of system-level objects is also collected for Security System-level Objects, Device and Credentials System-level Objects, Device Containment System-level Object, Automation Library (Compliance and Standardization) System-level Objects.

NCM records change of both the user who made the change and the user who approved the change in its revision history, including time stamp as detected either from the scheduled job, the change notification, or the device itself.

All audit trail entries are also recorded for both success and failure status such as DeviceRevChangeFailedEvent, DeviceRevCreateFailedEvent, DeviceRevPolicyCheckFailedEvent, CommunicationRestoredEvent, etc...
NCM categorizes each event by action type, event type, severity type, and source type. The action type is the actual type of event, such as JobFailedEvent.

To synchronize all critical system clocks and times, a template called Test For Network Time Protocol can be used.

Securing audit trails to avoid altering can be done with NCM as well. Users are constrained to only see events for resources to which they have view permissions. NCM has a system-level permission named View Audit which controls whether a user may see event logs.

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

12.1, 12.1.1 The Archer/NCM integration can be used to publish the process documentation written by the user. This process documentation is useful not only for dissemination across the group but also for daily review by engineers responsible for certain aspects of PCI.

Users and auditors can also get a focused view of the requirements, best practices, samples and reports to help engineers address each requirement. The integration will help engineers stay well informed as to the requirements of PCI and the compliance status of the network.

**Table 3. PCI DSS 2.0 Applicability Matrix for VMWare vCenter Configuration Manager**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Controls Addressed</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirement 2:</strong> Do not use vendor-supplied defaults for system passwords and other security parameters</td>
<td>2.1.1, 2.2.1, 2.2.2, 2.2.3, 2.2.4</td>
<td>vCM can be used to detect, and in many circumstances, correct default security settings on Windows, Solaris and Linux systems. System security parameters can be configured following hardening guideline for Windows, Solaris and Linux. Admin can also remove unnecessary functionality via built-in remediation actions as well as scripted remote commands.</td>
</tr>
<tr>
<td><strong>Requirement 5:</strong> Use and regularly update anti-virus software or programs</td>
<td>5.1, 5.2</td>
<td>Although vCM is not an anti-virus solution, it can be used to assess and report the anti-virus state of the system. This allow a determination that all systems have anti-virus software installed and running with the updated signature files.</td>
</tr>
<tr>
<td><strong>Requirement 6:</strong> Develop and maintain secure systems and applications</td>
<td>6.1</td>
<td>vCM is able to access, download and deploy patches to Windows, Unix, Linux and Mac operating systems. Assessments are customizable and can be set to verify critical patches in the past 30 days. Changes within the virtual environment are captured as well. Each change made to the configuration settings is</td>
</tr>
<tr>
<td>Requirement</td>
<td>Description</td>
<td>Requirement Details</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>Requirement 7:</strong> Restrict access to cardholder data by business need to know</td>
<td></td>
<td>vCM can be used to validate user access to data stored on any Windows, Solaris and Linux system.</td>
</tr>
</tbody>
</table>
| **Requirement 8:** Assign a unique ID to each person with computer access | 8.1, 8.2, 8.5.1, 8.5.4, 8.5.5, 8.5.6, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 | vCM has the ability to monitor access controls and report on the following:  
  - Local and domain-level users (Windows) and users with unique username (UNIX, Linux and Mac).  
  - System password policies for expiration, length, standards, creation settings, and access attempts  
  - Changes to user accounts, credential stores, and identifier objects to provide visibility and control over system access  
  - User access across all the systems in the datacenter at once  
  - Disable and remove access for terminated user accounts  
  - Inactive accounts (which it can also disable and remove access for these user accounts)  
  - The status of maintenance accounts and to confirm that they are disabled and configured to only be used during the times specified  
  - Login policies, to include lockout settings and auto-logout settings, and remediating as needed. Assessment, reporting and remediation is conducted in accordance with scheduling through vCM |
| **Requirement 10:** Track and monitor all access to network resources and cardholder data | 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.4, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5 | vCM will assess, report and remediate the following:  
  - Configurations of the system auditing and logging services to support proper logging across system components  
  - Collect audit logs entries to provide a single view of events  
  - NTP settings and configuration details  
  - User access audit trails by ensuring proper permissions for log files and their directories and alert on changes to critical audit trails |
| **Requirement 11:** Regularly test security systems and processes | 11.5 | vCM can be configured to monitor critical files and provide alerts and reports detailing any changes made or attempted. |