CHAPTER 5

Compliance

Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business. Violations of regulatory compliance regulations often result in regulatory actions, including federal fines, and the possibility of litigation.

There are different regulatory compliance laws for different market verticals, such as the following:

- For credit card data, the PCI DSS is a regulation that organizations who process such information must adhere to
- For the health care segment, the HIPAA is a requirement
- Federal agencies and their service providers must adhere to the FISMA

Regulatory compliance not only creates a defense against the threat, but it also offers an opportunity to consistently strengthen your organization through strategic, proactive measures-such as best practices, employee training, internal technical and process controls.

Virtualization is a significant movement within IT environments that enables many organizations to reduce storage and processing costs while simplifying overall management and improving scalability. It does provide the improvement and efficiency of their workloads but on the other side it has a dependency on the hardware platform it is built on and the security of that hardware in terms of access and control. There are many degrees of virtualization, but all create a virtual representation of an operating system, server, storage device, or network resource in order to abstract operations from physical devices.

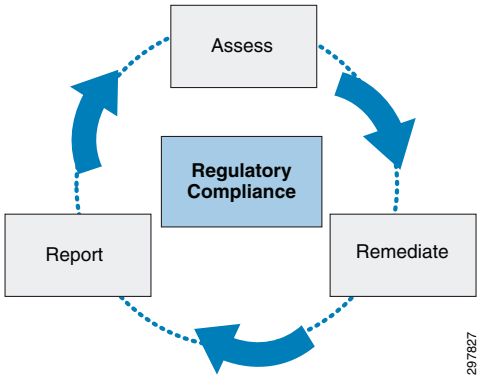
Virtualization has generated a trend toward cloud computing environments in which data, applications, and software based network overlay infrastructure can reside anywhere and services are delivered where needed, as needed, on demand to any device or end user.

Public clouds enable organizations to reduce their capitalized IT infrastructure, as well as management costs and complexity, by storing assets on a shared, but secured, hosted infrastructure. Enterprises can also build their own private clouds, with data center environments that can deliver cloud-based services within their own organization.

As there are benefits of public cloud and virtualization world, there are unique challenges, including but not limited to segmentation, data storage, access control, forensic auditing, logging, monitoring and alerting across complete network paradigm.

Compliance is not a one-time process, rather it is a continuous cycle of assessing the environment, re-mediating the issues, and then reporting and filing it.

Figure 5-1 Compliance Process Cycle



Although achieving compliance requires more than just technology, the network is critical in supporting organizations' compliance strategies. Cisco VMDC Cloud Security 1.0 offers a Unified Compliance Solution Framework with guidelines that facilitate addressing multiple regulatory compliance requirements from one network infrastructure. When working with the network, it is essential to address the scope of the compliance. The cost of compliance and complexity increases in proportion to the scope. Certain techniques and guidelines are provided on how to minimize the scope of the compliance more effectively and efficiently. There are some common themes among various compliance objectives, such as segmentation of traffic among tenants, identity and access control, and encryption of data at rest and in motion.

For example, it is recommended to use secure HTTP (HTTPS) and secure shell (SSH) Protocol that are secure replacements for the HTTP and Telnet protocols. The replacement protocols use secure sockets layer (SSL) and transport layer security (TLS) to provide device authentication and data encryption. These protocols are encrypted for privacy, and the unsecured protocols—Telnet and HTTP—are turned off on all the devices within the reference architecture.

In general there is a cost associated with achieving compliance that should be balanced against a potentially much larger set of costs if the organization is non-compliant.

Compliance Cost

Providing regulatory compliance on a cloud deployment infrastructure requires a larger initial investment for service providers. The following list shows a few areas where compliance can increase costs.

1. Technologies
2. Audits (Internal & External)
3. Remediation
4. Training
5. Management
6. Implementation

Other areas that can increase cost include proper processes, physical security, policies and planning.

Cost of Non-Compliance

As stated above, there are various factors that incur cost for achieving compliance as well as factors that incur much higher cost for non-compliance. Some of the key factors are shown below:

1. Significant Fines and Fees
2. Reputation of the service provider

3. Loss of production
4. Revenue Impact
5. Customer Relationship
6. Litigation or Arbitration Settlement Costs

To help reduce the risk of non-compliance, VMDC Cloud Security facilitates a service provider to achieve compliance for their cloud deployment in a more efficient manner by providing guidance and gap analysis in all three vertical deployments.

PCI DSS 3.0 Compliance Guidance

The PCI Data Security Standard (PCI DSS) provides guidance for securing payment card data. It includes a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS provides an actionable framework for developing a robust payment card data security process, including prevention, detection, and appropriate reaction to security incidents.

PCI Version 3.0 introduces new changes to the standard. The core 12 security areas as shown below are remain the same, but the updates include several new sub-requirements that did not exist previously. PCI version 2.0 will remain active until December 31st 2014 and organizations are required to comply with PCI, and PCI DSS version 3.0 officially goes into full effect on January 1, 2015 (Table 5-1).

Table 5-1 Service Provider Goals and PCI DSS Requirements

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

The PCI 3.0 new requirements are:

1. Lack of education and awareness
2. Weak passwords, authentication
3. Third-party security challenges
4. Slow self-detection, malware
5. Inconsistency in assessment

PCI DSS 3.0 changes are designed to help organizations take a proactive approach to protect cardholder data that focuses on security, not compliance, and makes PCI DSS a business-as-usual practice.

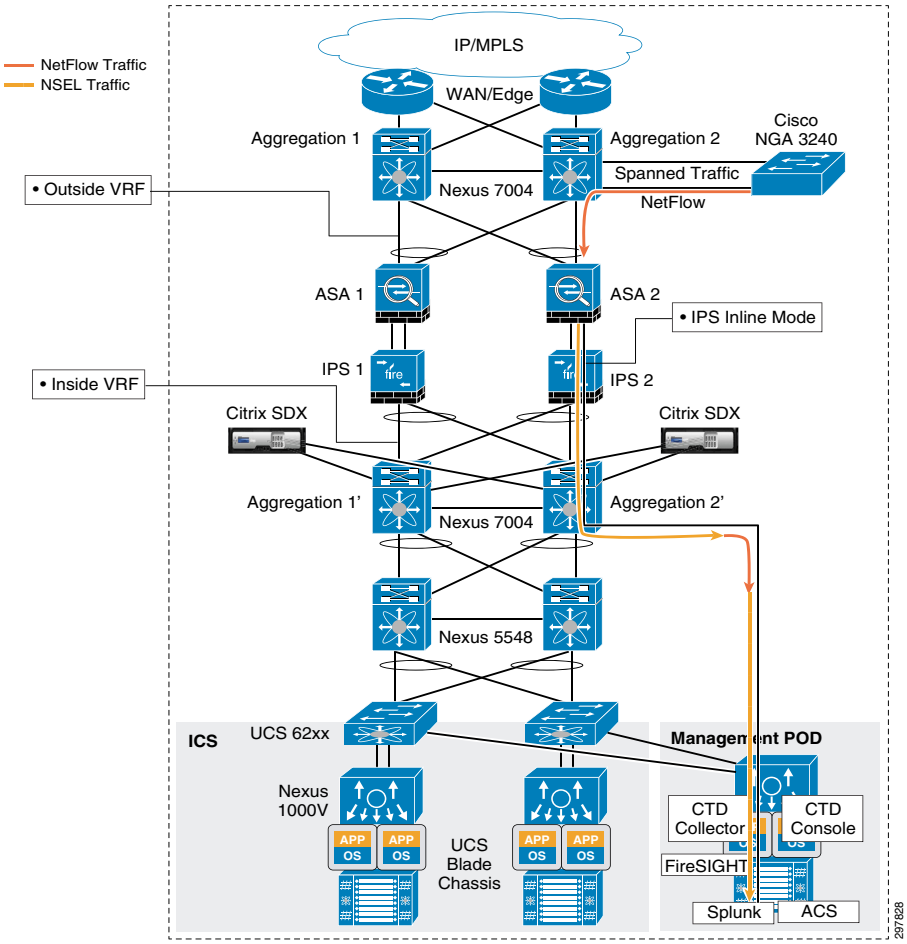
To overcome the challenge to meet these requirements, the VMDC Cloud Security 1.0 architecture includes next generation IPS, centralized password and authentication service, intelligent monitoring and network visibility tools such as Splunk and Cisco CTD, as described in the detail design section earlier in this document.

When service provider delivers cloud-based services to organizations such as financial institutions or organizations that store, process, or transmit cardholder data, those consumers are required to be compliant with PCI. However, not all organizations are required to meet the same number of controls. Control requirements are based on annual volume of credit card transactions, and the manner in which these credit cards are processed, transmitted, and/or stored. In some cases, the organization has the ability to self-assess for PCI Compliance. Organizations that process over six million transactions per year must have an annual assessment completed by a Security Assessor (independent third party or internal resource which has been approved by the PCI Security Standards Council).

In a multi services and multi-tenant cloud data center deployment model, the intelligent centralized log management is a key element for attaining PCI compliance. Cisco collaborated with technology partner Splunk to gather and aggregate logs from various components of the network and provide real time security event analysis and history of log management that can assist in a forensic investigation.

One of the greatest challenges to maintaining compliance the scope of the data center environment because if the service provider maintain their entire data center environment, it may not meet the PCI scope standards. A large scope may have devices and components that do not need to comply, but once in the scope, the PCI standards require these devices to be evaluated and audited. Figure 5-2 shows the layout of a complete data center network scope.

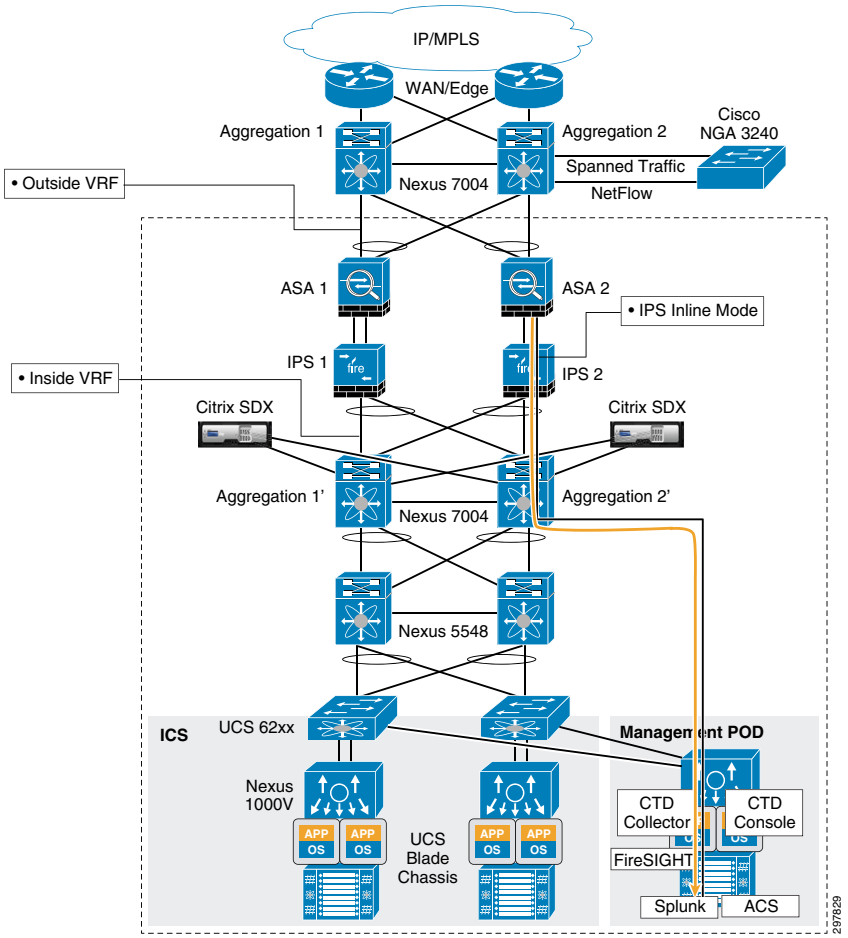
Figure 5-2 Scope of a Complete Data Center Network



As shown above, a service provider can bring in the 3rd party auditors to audit the entire data center including the NGA (Netflow generator appliance), WAN edge PE, and North VRF of Nexus 7K. This increases the scope of the PCI audit to include components outside the compliance scope. When scoping out network components within a data center, understanding the network and information flow is the primary step before properly selecting components.

In the network diagram above, there are various locations from where the security data has been collected, such as NetFlow traffic from Nexus 7K aggregation using NGA, and NSEL traffic from ASA, to the logging and monitoring device Splunk. The data collected from N7K and ASA are redundant in nature, due to the fact that all the customer traffic goes through the ASA firewall and thus, NetFlow traffic can be eliminated from the PCI scope, as shown in Figure 5-3.

Figure 5-3 Traffic Flow Through the ASA Firewall



In VMDC cloud security architecture, we have narrowed the scope to a limited section of the data center and eliminate the components that may not be required for PCI compliance.

Limiting the scope of the data center from a PCI perspective, as shown above, provides the ability for the VMDC cloud security architecture to achieve compliance efficiently.

PCI DSS 3.0 technical Control Mapping to VMDC Cloud Security 1.0 reference architecture is provided in Table 5-2.

Note This mapping is done based on the external audit with reference to the 12 major PCI DSS 3.0 requirements mentioned earlier.

Table 5-2 Mapping PCI DSS 3.0 to VMDC Cloud Security Reference Architecture

PCI DSS 3.0 Requirements	Total Controls	Controls Assist by VMDC	Controls Directly Achieved by VMDC	Product
Requirement 1	37	23	14	ACS, ASA, Splunk, BMC,
Requirement 2	30	13	0	Splunk, IPS, BMC
Requirement 3	44	Not Applicable	Not Applicable	Not Applicable

Table 5-2 Mapping PCI DSS 3.0 to VMDC Cloud Security Reference Architecture (continued)

PCI DSS 3.0 Requirements	Total Controls	Controls Assist by VMDC	Controls Directly Achieved by VMDC	Product
Requirement 4	11	Not Applicable	Not Applicable	Not Applicable
Requirement 5	11	Not Applicable	Not Applicable	Not Applicable
Requirement 6	44	3	1	IPS, VMDC Release Process
Requirement 7	10	9	0	ACS
Requirement 8	43	32	2	ACS, ASA
Requirement 9	45	Not Applicable	Not Applicable	Not Applicable
Requirement 10	41	35	3	Splunk, NTP server, N7K, N5K, ASA
Requirement 11	32	5	5	IPS, Splunk
Requirement 12	47	Not Applicable	Not Applicable	Not Applicable
Total	**395**	**120**	**25**	

For further details, refer to the Cisco Design Zone VMDC landing page.

Note The completion of a PCI DSS 3.0 assessment or guidance alone will not prevent a compromise of data. This information only addresses the capability of compliance for VMDC Cloud Security 1.0 reference architecture against PCI DSS 3.0 security requirements as published. Recommendations within this guidance are intended only to aid in compliance against the assessed control baselines and prioritized based on perceived business requirements.

HIPAA Compliance Guidance

VMDC Cloud Security 1.0 reference architecture provides guidance and tactical designs for HIPAA compliance. It clarifies how the data center network components can address requirements when a service provider delivers services to health professional or health related enterprises.

The HIPAA Omnibus Final Rule, released in January 2013, included updates from the Health Information Technology for Economic and Clinical Health (HITECH) Act, breach notification, penalty tiers, and extended HIPAA compliance obligations to include both covered entities and business associates. Any transaction that includes reception, transmission, storage or processing of protected health information (PHI) in electronic format need to comply with the HIPAA standards.

The VMDC Cloud Security 1.0 reference architecture uses the National Institute of Standards and Technology (NIST) publication 800-66, revision #1 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. NIST 800-66 encompasses requirements for Healthcare organizations and their downstream partners to ensure security and privacy of electronic Protected Health Information (ePHI).

Note NIST 800-66 control set applies solely within the United States in the form of the Health Insurance Portability and Accountability Act (HIPAA). While HIPAA is a United States statute, VMDC Cloud Security 1.0 reference architecture is versatile and supports configurations to meet stringent security and privacy requirements as they apply to International or Non-United States based entities.

The service provider - when deploying the data center for providing services to healthcare enterprises - may be required to meet certain administrative, physical and technical safeguards as described by the US Department of Health and Human Services.

The HIPAA Omnibus Final Rule consists of three main sections:

- **Part 160**—General Administrative Requirements. Deals mostly with the legal, compliance, and penalty aspects of HIPAA.
- **Part 162**—Administrative Requirements. Deals with unique identifiers for covered entities in healthcare, provisions for transactions, and many other administrative issues in healthcare.
- **Part 164**—Security and Privacy. Deals with the safeguards for protecting PHI in electronic and paper media. Part 164 consists of the following:
  - **Subpart A**—General Provisions §164.1xx
  - **Subpart B**—Reserved
  - **Subpart C**—Security Standards for the Protection of Electronic Protected Health Information §164.3xx
  - **Subpart D**—Notification in Case of Breach of Unsecured Protected Health Information §164.4xx
  - **Subpart E**—Privacy of Individually Identifiable Health Information §164.5xx

Note From infrastructure perspective, the VMDC Cloud Security 1.0 reference architecture is primarily focused on Part 164 subpart C (§164.3xx).

The VMDC Cloud Security 1.0 reference architecture does not guarantee HIPPA compliance; rather it facilitates and provides guidance for achieving compliance. The responsibility for compliance is always on the data owner.

Table 5-3 shows the mapping of the HIPAA rule controls to VMDC components. It should be noted that there are many controls under each section. For example, under 164.312 rule, there are more than 20 controls.

For details about the complete list of controls, service provider needs to review the HIPAA compliance standards.

Table 5-3 HIPAA Control Mapping to VMDC Cloud Security Reference Architecture

HIPAA RULE	VMDC Facilitate	VMDC Directly Support	Product
164.310(b)	Yes		N7K, N5K, ASA, IPS, FI, UCS, ACS, NGA, Cisco CTD, Splunk Storage, Server Blades
164.310(d)(1)	Yes		Server Blades, ESXi, VMware
164.312(a)(1)		Yes	ACS
164.312(a)(2)(i)		Yes	ACS
§164.312(a)(2)(ii)		Yes	ACS, Splunk
§164.312(b)		Yes	Splunk
§164.312(c)(1)		Yes	ACS
§164.312(c)(2)		Yes	Splunk, IPS
45 CFR § 164.304		Yes	ACS

Table 5-3 HIPAA Control Mapping to VMDC Cloud Security Reference Architecture (continued)

HIPAA RULE	VMDC Facilitate	VMDC Directly Support	Product
§164.312(d)		Yes	ACS
§164.312(e)(1)		Yes	ASA, SSL VPN
§164.312(e)(2)(i)		Yes	ASA, VPN
§164.312(e)(1)(ii)		Yes	ASA, VPN

There are four major categories that reduce the risk of losing control over PHI data:

- Segmentation, page 5-9
- Identity and Access Management, page 5-9
- Logging, Auditing, and Monitoring, page 5-10
- Encryption and Decryption, page 5-10

Segmentation

Segmentation is a basic building block when becoming HIPAA compliant. In a multi-tenant cloud deployment model, the service provider needs to ensure all tenants are completely segmented into their individual containers. In some cases within an enterprise, segmentation and isolation is required from HIPAA perspective, especially if one department is dealing with PHI data and others are not. The VMDC Cloud Security 1.0 reference architecture built the segmentation and isolation of each tenant end-to-end, using techniques like Layer 3 VRF, Layer 2 VLAN, separate firewall context, VSAN and intra-tenant segmentation VSG. This segmentation using switches may apply to the HIPAA Safeguard for guarding against malicious software as described in 164.308(a)(5)(ii)(B).

The need to segment, separate, and isolate administrative and PHI data is huge in limiting the scope and depth of security controls that are applied for HIPAA compliance. By segmenting PHI data from administrative information, service providers can protect PHI data by applying the appropriate controls. Proper segmentation and QoS play a key role in terms of hosting a health care provider. Huge files, such as imaging, xrays, can be transferred across a server safely and rapidly.

Firewalls also play a key role in segmenting the traffic and protecting PHI data. The Access Control Lists (ACLs) provide explicitly permitted and/or denied IP traffic that may traverse between inside, outside, and DMZ zones. Routing and access control lists provide segmentation between authorized and unauthorized access on the network. This capability can be mapped to the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i); and protecting ePHI from parts of an organization that are not authorized such as Isolating Healthcare Clearinghouse Functions 164.308(a)(4)(i).

Identity and Access Management

VMDC Cloud Security 1.0 reference architecture recommends the centralized identity and access management using Cisco ACS server. Cisco Secure Access Control System (ACS) is a highly scalable, policy-based network access and device access administration control platform that centralizes:

- Network device administration control
- Flexible and granular user authentication and authorization control
- Controls network and device access based on dynamic conditions and attributes

- Access to multiple Identity Databases, both internal and external such as Active Directory

Identity management, authentication, authorization, and access control of users and systems to PHI is the central theme in the HIPAA Security Rule safeguards. A strong and manageable identity and access control solution is critical for achieving an assessment finding of a low level of risk under a risk management program in HIPAA.

As mentioned above, Identity Management should be centralized from the compliance perspective, however in case of failure of the centralized system, compliance requirements may specify that local identity and access management be configured for emergency access. For example, if an ACS server went down and a health professional needed to access a certain critical application, the service provider administrator should be able to provide some emergency access. This ensures that the ability to control system access during both routine and emergency events is supported. The HIPAA security rule 164.312.(a)(1) Access Control requires that technical policies and procedures be implemented to allow access only to authorized persons or software programs. All non-authorized personnel should not have access even during the potential failure of the centralized authorization service.

Logging, Auditing, and Monitoring

A particularly critical requirement of the HIPAA Security Rule is the logging, auditing, intrusion detection and monitoring of PHI data within the service provider environment. In this reference architecture, Splunk plays a key role as a centralized component for collecting application, database, device and user access logging as well as the enablement of auditing that is critical to effectively supporting a service provider or business associates breach management strategy. For HIPAA compliance, real time intrusion detection and protection of all the tenants that generate PHI or ePHI data is paramount, especially in a large and complex data center deployment such as the VMDC Cloud Security 1.0 reference architecture, where such intrusions and malware may become breaches if not detected in a timely fashion. To provide such services, the reference architecture uses NextGen IPS that detects and applies deep packet analysis and inspection at line rate. It performs the following:

- Access global intelligence with the proper context to make informed decisions and take immediate action.
- Consistently enforce policies across the entire network and have the control to accelerate threat detection and response.
- Detect, understand and halt advanced malware/advanced persistent threats across the entire attack continuum.

For example, the IPS/IDS identify, protect or block individuals or data that post suspicious activity within the data center. This falls under the HIPAA requirement for identifying and responding to suspected or known security incidents (164.308(a)(6)(ii)).

Logging, auditing, and monitoring are critical factors for a service provider to meet HIPAA Accounting Rule 164.528, and can help identify whether a compromise has occurred that may lead to a breach notification.

As mentioned above, the logging should be centralized, but to meet compliance in case of centralized system failure, the logging should be enabled on each of the HIPAA scoped components locally.

Encryption and Decryption

According to the HIPAA Security Rule, the PHI data must be kept secure during transmission under the addressable implementation specification for encryption. There should be application layer encryption, but additional consideration should be given when PHI leaves the health related enterprise, such as

clinics over Internet service provider (VPN). For example, in this reference design, the recommendation is to have SSL VPN between end customers and the service provider cloud data center where the services are deployed. To protect the PHI data and prevent unnecessary exposure, encryption and decryption plays a most effective role. This enables service providers to meet the HIPAA Safeguard 164.312(a)(1)(2)(iv) Encryption and Decryption. Providing encryption of traffic over public networks meets the HIPAA requirement for Transmission Security 164.312(e)(1), Integrity 164.312(e)(2)(i), and Encryption 164.312(e)(2)(ii).

Typically, when healthcare-related tenants transmit PHI data over the Internet to the centralized data center, is the data is secured as a demilitarized zone (known as DMZ). In this reference architecture, firewall and IPS are used to provide a DMZ zone for all Internet access from any healthcare related tenants.

Details on how to create DMZ zone within the VMDC Cloud Security 1.0 reference architecture can be found using the link below:

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/2-3/design_guide/VMDC_2-3_DG.pdf

Note The completion of a HIPAA assessment or guidance alone will not prevent a compromise of data. This information addresses only the capability of compliance for VMDC Cloud Security 1.0 reference architecture against HIPAA security requirements as addressed by NIST. Recommendations within this guidance are intended only to aid in compliance against the assessed control baselines and prioritized based on perceived business requirements.

FISMA Compliance Guidance

Title III of the E-Government Act, also known as FISMA, requires federal agencies or their service providers to implement risk-based information security programs. The National Institute of Standards and Technology (NIST) provides the Risk Management Framework in a series of Federal Information Processing Standards (FIPS) and special publications.

To meet compliance requirements of the Federal Information Security Management Act (FISMA), service providers and federal agencies must include planning, processes, and technology together to make effective use of resources and money while protecting the confidentiality, integrity, and accessibility of mission-critical information systems.

To aid in both cost-effectiveness and risk-based decision making, information systems are categorized based on the type of information being processed. The resulting categorization is then utilized to select the appropriate security controls to be implemented. Once implemented, the controls are assessed and if appropriately applied, are authorized for operation within the federal sector. Continuous monitoring activities take place to ensure security controls continue to operate and provide sufficient protection.

Without a thorough understanding of FISMA and security control implementations, many solutions do not integrate FISMA compliance into their development life cycles. Without security integration, configuring solutions to comply with FISMA becomes a complicated and tedious process contributing to excessive financial and labor costs. Organizations will find implementing new solutions into an existing architecture is similar to fitting a square peg into a round hole for each individual control. In some instances, system customization must be performed to meet requirements. These complications add onto an existing high-dollar compliance program.

The Self-Defending Network is Cisco's strategy to protect federal organizations from security threats caused by both internal and external sources. This protection enables government agencies and their service providers to take better advantage of the intelligence in network resources, thus improving overall security while addressing FISMA requirements.

The VMDC Cloud Security 1.0 solution can facilitate service providers to meet FISMA requirements, including mitigations for unauthorized access, malicious code, scans and probes, improper usage, and denial-of-service attacks.

Challenges and Guidance

In an increasingly dynamic environment facing advanced persistent threats, the challenge of effectively achieving and maintaining FISMA compliance can be significant. Within a data center, virtualization is another key challenge that can delay and jeopardize compliance if not properly deployed with various security controls.

The biggest challenge with FISMA is that most organizations do not have personnel that fully understand the FISMA compliance process. The NIST recommended controls are very non-prescriptive and thus are not easily understood by typical IT staff. This means that the already time consuming task of working towards FISMA compliance becomes almost impossible with inexperienced staff.

Another challenge is that there are no “out of the box/off the shelf” solutions to ensure compliance with specific technical controls. Most hardware and software put into place have to be meticulously configured in a way that is not covered in the manufacturer’s guide to meet the control requirements. Configuring the hardware and software considered in scope for FISMA compliance requires extra time to research, test, and implement these changes, all while still being unsure whether or not it’s actually meeting the requirement.

The FISMA Gap Assessment process focused on the security of information systems by determining whether Cisco has effectively implemented the capabilities required to apply adequate security measures that comply with the requirements as outlined by NIST.

VMDC Cloud Security 1.0 reference architecture was assessed against a moderate impact baseline. 86 of 265 controls were applicable, including controls within Access Control, Audit and Accountability, Identification and Authentication, System and Services Acquisition, System and Communication Protection, and System and Information Integrity families.

Implementation

The VMDC Cloud Security 1.0 reference architecture assessment found all 86 of the controls identified above as being satisfied when an organization implements the Cisco VMDC architecture in accordance with Cisco's configuration documentation. These controls aid service providers by providing guidance with numerous NIST control families including Access Control, Audit and Accountability, Identification and Authentication, System and Services Acquisition, System and Communication Protection, and System and Information Integrity. Leveraging the technical controls defined by and audited within the Cisco VMDC architecture provides better guidance for service providers who need to meet the FISMA requirements.

Integration of the VMDC solution into a FISMA compliant architecture will allow service providers, large enterprises, and federal agencies to mitigate impacts on two levels: system integration, and system management. Service providers deploying VMDC 2.x-based reference architecture are capable of implementing predefined configurations that are known to be compliant, and more importantly, secure, using Cisco best practices and recommendations.

During the FISMA audit, auditors subject the VMDC solution to a rigorous assessment that resulted in 86 security controls for direct implementation. The second level of impact exists where organizations have the capability of integrating the VMDC solution into a secure environment and adapting existing operational and management controls. This two-tiered benefit achieves FISMA alignment for secure system integration and management within the environment.

The VMDC Validated Design feature enables a transparent network flow from the physical to the virtual network, enabling agile operations and simpler management. It can create multiple security zones that logically separate tenant resources from one another in the virtual network and allow fault-tolerant virtual machine movement. Edge security protects the data center from external threats and offers secure contextual access to data center resources. The NextGen IPS provides deep packet inspection and blocks all possible cyber threats before they can impact the network. Similarly the network visibility tools and log monitoring help service providers to see the full picture of their network continually to better enable proactive management in a timely fashion. All of these security features within VMDC provide a seamless mapping and integration of FISMA controls.

Considerations

The Federal Information Security Management Act (FISMA) framework establishes baseline security criteria for all Federal Agencies and contractors for the United States Government. Currently the standard is on Revision 4 and applies solely within the United States. Applicable only within the United States, many common requirements are shared by International Standards. The reference architecture is a versatile solution and supports configurations to meet stringent security and privacy requirements as they apply to international or non-United States based entities.

FISMA Compliance & VMDC Cloud Security Reference Architecture Mapping

There are various areas that FISMA requires to be addressed before any organization attempts to attain FISMA compliance. A summary of the VMDC solution's ability to meet such compliance requirements are shown in the table below. There are controls from various sections of FISMA guidance that may not apply to directly to VMDC. For example: training and awareness for information security personnel, maintenance, and physical protection for the network and data center.

With all the complexity surrounding FISMA, organizations can find the compliance process challenging. VMDC alleviates obstacles by taking care of the majority of the most difficult technical requirements to implement. By using VMDC, organizations can focus their efforts on the operational and management controls associated with FISMA, allowing them to move quickly through the compliance process.

Several tools are available within the VMDC environment to help facilitate FISMA compliance; including ASA firewalls, Cisco FirePOWER IDS/IPS, Lancope StealthWatch, Cisco ACS, and Splunk.

Customized ASA firewalls are used to properly segment each organization's FISMA boundary from other environments. Firewalls are required between any FISMA and non-FISMA environment per the System and Communication Protection family of FISMA controls.

Splunk, which is Security Information and Event Management (SIEM) software, covers many of the FISMA controls within the environment, including the Audit and Accountability family of controls. Audit and Accountability requires the use of a centralized log server that has the ability to discover and alert upon anomalies within the logs.

The Cisco FirePOWER Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) monitor both inbound and outbound network traffic. If anomalies are found throughout the monitoring process, Cisco FirePOWER can be configured to email an organizational resource an alert when it has identified malicious traffic. For specific types of anomalies, the IPS function of the appliance will automatically

identify attack signatures and prevent the malicious traffic from occurring in the future. This layer of security helps cover requirements across all areas, but mainly assists in the implementation of controls within the System and Communication Protection family of FISMA controls.

Cisco CTD uses network device telemetry to provide deep, complete visibility across the network core, enabling security operators to understand and use network traffic details to discover anomalies. Deploying Cisco CTD across networks can provide information and visibility to support security operators in a variety of threat detection tasks, including:

- Data loss detection
- Network reconnaissance of internal networks
- Monitoring the spread of malware in internal networks
- Botnet command and control channel detection in internal networks

Implementation of Cisco CTD assists in meeting FISMA requirements mainly from Audit and Accounting and Incident Reporting that include forensic audit capability.

Cisco Secure Access Control Server (ACS) is a highly scalable, high-performance access control server that operates as a centralized RADIUS and TACACS+ server. It extends access security by combining authentication, user access, and administrator access with policy control within a centralized identity networking solution, allowing greater flexibility and mobility, increased security, and user-productivity gains.

Cisco Secure ACS enforces a uniform security policy for all users regardless of how they access the network. It reduces the administrative and management burden involved in scaling user and administrator access to the network. By using a central database for all user accounts, Cisco Secure ACS centralizes the control of all user privileges and distributes them to hundreds or thousands of access points throughout the network.

Cisco Secure ACS provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications. It helps to ensure enforcement of assigned policies by allowing network administrators to control:

- Who can log into the network
- The privileges each user has
- Security audit or account billing information
- Access and command controls for each configuration's administrator

Cisco Secure ACS addresses concerns about compliance by supporting features associated with administrator permission and audit reports:

- Administrative constraints on log settings restrict administrators from disabling certain types of logging.
- Forced administrator password change at login prompts administrators to change the password at configurable time intervals.
- Administrator password policy provides a mechanism to enforce a configurable minimum password length and mix of characters (upper/lower case, numeric, punctuation).
- Forced administrator password change for stale account enforces password change when the administrator has not logged on in for a specified number of days.
- Generation of entitlement reports provides a report that shows all administrator privileges.
- Password history for administrators prevents reuse of passwords.

ACS helps service provider to meet FISMA requirements in multiple areas such as Access control, Audit and Accounting, Risk Management and Identification and Authentication.

Table 5-4 FISMA Control Mapping to VMDC Cloud Security Reference Architecture

Compliance Section Number	Section Title	Total Controls	Controls Facilitated by VMDC	Product Mapping
AC	Access Control	35	19	ACS, IPS, Nexus Switches, ASA, Cisco CTD, SPlunk
AT	Awareness and Training	5	0	Not Applicable
AU	Audit and Accounting	17	10	ACS, Splunk, Cisco CTD, IPS
CA	Security Assessment and Authorization	10	2	ASA, IPS, Splunk
CM	Configuration Management	19	7	ASA, IPS, BMC management tool
CP	Contingency Planning	23	4	MDS, NetApp
IA	Identification and Authentication	22	13	ACS, ASA, All products with password complexity
IR	Incident Response	12	2	Splunk, Cisco CTD, IPS
MA	Maintenance	10	0	Not Applicable
MP	Media Protection	9	1	NetApp
PE	Physical and Environment Protection	20	0	Not Applicable
PL	Planning	6	0	Not Applicable
PS	Personnel Security	8	1	Splunk
RA	Risk Assessment	7	1	ACS
SA	System and Services Acquisition	14	1	VMDC documentation
SC	Systems and Communication Protection	27	17	ACS, N7K, N5K, IPS, ASA, NetApp,
SI	System and Information Integrity	21	8	Splunk, IPS
Total		**265**	**86**	

For further details, refer to the Cisco Design Zone VMDC landing page.

Note The completion of a FISMA assessment or guidance alone does not prevent a compromise of data. This guide addresses only the capability of compliance for VMDC Cloud Security 1.0 reference architecture against FISMA security requirements as published by NIST. Recommendations within this guidance are intended only to aid in compliance against the assessed control baselines and prioritized based on perceived business requirements.

Benefit of VMDC Cloud Security Guidance towards FISMA Compliance

Specific benefits include:

1. **Demonstrated solutions to critical technology-related problems in evolving IT infrastructure—**Provides support for cloud computing, applications, desktop virtualization, consolidation and virtualization, and business continuity.
2. **Reduced time to deployment—**Provides best-practice recommendations based on a fully tested and validated architecture, facilitating technology adoption and rapid deployment.
3. **Reduced Risk—**Enables enterprises and service providers to deploy new architectures and technologies with confidence.
4. **Increased Flexibility—**Provides rapid, on-demand, workload deployment in a multi-tenant environment using a comprehensive automation framework with portal-based resource provisioning and management capabilities.
5. **Improved Operating Efficiency—**Integrates automation with a multi-tenant pool of computing, networking, and storage resources to improve asset use, reduce operation overhead, and mitigate operation configuration errors.