HyTrust Addendum to the VMware Product Applicability Guide

For

Federal Risk and Authorization Management Program (FedRAMP) version 1.0

August 2014
# Table of Contents

EXECUTIVE SUMMARY ............................................................................................................................................ 3  
INTRODUCTION ......................................................................................................................................................... 4  
OFFICIAL FEDRAMP GUIDANCE AS IT APPLIES TO CLOUD ENVIRONMENTS ............................................. 5  
CLOUD COMPUTING.................................................................................................................................................. 10  
WHERE TO START – CONSIDERATIONS FOR SYSTEM OWNERS, IT AND ASSESSORS ........................... 12  
GUIDANCE FROM THE FEDERAL RISK AUTHORIZATION MANAGEMENT PROGRAM ................................. 13  
HYTRUST TECHNOLOGIES AND FEDRAMP ......................................................................................................... 14  
HYTRUST FEDRAMP REQUIREMENTS MATRIX (OVERVIEW) ........................................................................ 15  
  
  HyTrust Boot Attestation Service with Intel TXT .................................................................................................. 15  
  INTEL TXT ......................................................................................................................................................... 15  
FEDRAMP REQUIREMENTS MATRIX (BY HYTRUST PRODUCT) ........................................................................ 16  
  
  HyTrust CloudControl .............................................................................................................................................. 16  
  HyTrust DataControl ............................................................................................................................................. 21
EXECUTIVE SUMMARY

The Federal Risk Authorization and Management Program (FedRAMP) was created to provide a streamlined and standardized process along with a "do once, use many times" approach to the authorization of commercial cloud services. This program enables US Government agencies to take full advantage of the benefits of migrating their IT assets and infrastructure to the cloud, as they work to meet the goals of the Federal Cloud Computing Strategy published by the White House in February 2011. FedRAMP, which is governed by a Joint Authorization Board (JAB) that consists of representatives from the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense (DoD) is also endorsed by the U.S. government’s CIO Council including the Information Security and Identity Management Committee (ISIMC).

The FedRAMP program provides an avenue for Cloud Service Providers (CSPs) to obtain a provisional Authority to Operate (p-ATO) after undergoing an independent third-party security assessment that has been reviewed by the JAB, or by a sponsoring Agency. By assessing security controls on candidate platforms, and providing P-ATOs on platforms that have acceptable risk, FedRAMP significantly reduces the time and cost to agencies by removing the assessment and authorization requirements of the underlying cloud vendor services on a system-by-system basis. This minimizes the work each Consumer of FedRAMP Cloud resources must undergo to receive an actual ATO for the workloads running applications that process sensitive data and transactions.

For these reasons HyTrust has enlisted its Audit Partners such as Coalfire, a FedRAMP-approved 3rd Party Assessment Organization (3PAO), to engage in a programmatic approach to evaluate HyTrust products and solutions for FedRAMP control capabilities and then to document these capabilities into a set of reference architecture documents. The first of these documents in the FedRAMP Reference Architecture set is this document, the Product Applicability Guide, which contains a mapping of the HyTrust products and features that should be considered for implementing FedRAMP controls. The next two documents in the FedRAMP Reference Architecture set are the Architecture Design Guide and the Validated Reference Architecture. For more information on these documents and the general approach to compliance issues please review VMware's Approach to Compliance.

This study investigated different HyTrust applications available to organizations that use (or are considering using) VMware based virtualization and cloud services to support a FedRAMP compliant environment. To that end, Coalfire highlighted the specific FedRAMP requirements these applications (partially) address or should be considered in an evaluation of the initial sourcing of technologies to build a FedRAMP compliant environment. The controls selected for this paper are from the NIST SP 800-53 Rev3 and the FedRAMP Security Controls Baseline. It has been reviewed and authored by our staff of FedRAMP auditors in conjunction with HyTrust.

This Product Applicability Guide Addendum builds upon the base VMware control mapping and alignment for FedRAMP 1.0, which is documented in the VMware Product Applicability Guide for FedRAMP 1.0 on the VMware Solutions Exchange.

If you have any comments regarding this whitepaper, we welcome any feedback at vmware@coalfire.com or compliance-solutions@vmware.com.
INTRODUCTION

Compliance and security continue to be top concerns for organizations that plan to move any or their entire enterprise-computing environment to the cloud. HyTrust helps organizations address these challenges by providing bundled solutions (suites) that are designed for specific use cases. These use cases address questions like “How can I be FedRAMP compliant in a HyTrust supported vCloud hosting environment?” by providing helpful information for Virtualization architects, the compliance community, and third parties.

The FedRAMP compliant Public Cloud Use Case (See section on Cloud Computing in this document for Cloud Use Cases) is focused on the vCloud Service Provider intending to operate a FedRAMP compliant Public Cloud. Due to the nature of the Public Cloud Use Case this document is primarily concerned with guiding readers in the assembly of HyTrust components within the ‘Provider’ layer. This layer is comprised of HyTrust CloudControl and HyTrust DataControl. These product suites are described in detail in this paper and in the aforementioned subsequent companion documents. The use case also provides readers with a mapping of the specific FedRAMP controls to HyTrust’s product suite. While every cloud is unique, HyTrust, VMware and their partners can provide a solution that addresses over 19% of FedRAMP Moderate requirements with 70% of coverage among technical and operational controls.

FedRAMP is based on the NIST SP 800-53 Rev3 set of controls. While this document is intended to provide guidance solely within the Public Cloud Use Case it can also be beneficial to those who seek guidance on building a FISMA Moderate (NIST SP 800-53 Rev3) Private Cloud environment. Another version of the Reference Architecture written specifically for the FISMA Moderate Private Cloud Use Case is expected to be released later in 2014.

Due to the commonalities of the HyTrust products and features across all of the Cloud Use Cases, understanding their relationship to the seventeen FedRAMP control areas is fundamental and most broadly accommodated in this document with more Use Case specific guidance represented in the Architecture Design Guide. Regardless of the Use Case or operating environment model the FedRAMP control areas represent a broad-based, balanced, information security program that addresses the management, operational, and technical aspects of protecting federal information and information systems. The management, operational, and technical controls (i.e., safeguards or countermeasures) are prescribed for an information system in order to protect the confidentiality, integrity, and availability of the system and its information. The operational security controls are implemented and executed primarily by people (as opposed to systems). The management controls focus on the management of risk and the management of information system security. The technical security controls are implemented and executed primarily by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

A comprehensive assessment of the management, operational and technical controls that have been selected for the “information system” is required as part of the authorization process. This assessment must determine the extent to which all selected controls are implemented correctly, operating as intended, and producing desired outcomes with respect to meeting the security requirements for the system. An understanding of both FISMA Moderate and FedRAMP controls as implemented with VMware, HyTrust and their Technology Partners’ solutions lends itself to harmonizing the ongoing compliance of the private cloud environment but also the shared responsibility for compliance in the public cloud environment. This common set of well-understood policies and procedures implemented in a common HyTrust Software across Private and Public Cloud enables not only the Hybrid Cloud to become reality but opens up tremendous opportunities for tighter control and agility with regard to the principles put forth in the Continuous Diagnostics and Mitigation program as outlined by Department of Homeland Security.
OFFICIAL FEDRAMP GUIDANCE AS IT APPLIES TO CLOUD ENVIRONMENTS

The Federal Risk Authorization Management Program (FedRAMP) is the result of close collaboration with cybersecurity and cloud experts from GSA, NIST, DHS, DOD, NSA, OMB, the Federal CIO Council and its working groups, as well as private industry. The goal is to provide a streamlined process for the security assessment and authorization of commercial cloud services. This process allows a single Provisional Authorization (p-ATO) of the cloud service offering to be leveraged by any federal agency without requiring them to re-assess the hosting infrastructure on a per-system basis.

CSPs must implement the FedRAMP security requirements in their environment and hire a FedRAMP-approved third party assessment organization (3PAO) to perform an independent assessment to audit the cloud system and provide a security assessment package for review. In order to maintain a Provisional Authorization the cloud service provider must implement a continuous monitoring program. This is critical to ensuring the security controls outlined in the NIST SP 800-53 Rev3 controls and the additional FedRAMP parameters are effectively implemented.

The FedRAMP security controls baseline is based on the NIST SP 800-53 Rev3 controls that provide detailed Management, Operational and Technical control guidance for meeting the security requirements established by Federal Information System Management Act (FISMA). In addition to the FISMA compliance requirements outlined in the NIST controls baseline, FedRAMP requirements have been written for key controls and control enhancements.
Table 1: FedRAMP Controls Baseline

<table>
<thead>
<tr>
<th>NIST 800-53 Rev3 CONTROL FAMILY IDENTIFIERS</th>
<th>NIST 800-53 Rev3 CONTROL FAMILY</th>
<th>CLASS</th>
<th>FEDRAMP MODERATE BASELINE*</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Access Control</td>
<td>Technical</td>
<td>17(24)</td>
</tr>
<tr>
<td>AT</td>
<td>Awareness and Training</td>
<td>Operational</td>
<td>4</td>
</tr>
<tr>
<td>AU</td>
<td>Audit and Accountability</td>
<td>Technical</td>
<td>12(9)</td>
</tr>
<tr>
<td>CA</td>
<td>Certification, Accreditation, and Security Assessment</td>
<td>Management</td>
<td>6(2)</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
<td>Operational</td>
<td>9(12)</td>
</tr>
<tr>
<td>CP</td>
<td>Contingency Planning</td>
<td>Operational</td>
<td>9(15)</td>
</tr>
<tr>
<td>IA</td>
<td>Identification and Authentication</td>
<td>Technical</td>
<td>8(10)</td>
</tr>
<tr>
<td>IR</td>
<td>Incident Response</td>
<td>Operational</td>
<td>8(4)</td>
</tr>
<tr>
<td>MA</td>
<td>Maintenance</td>
<td>Operational</td>
<td>6(6)</td>
</tr>
<tr>
<td>MP</td>
<td>Media Protection</td>
<td>Operational</td>
<td>6(5)</td>
</tr>
<tr>
<td>PE</td>
<td>Physical and Environmental Protection</td>
<td>Operational</td>
<td>18(5)</td>
</tr>
<tr>
<td>PL</td>
<td>Planning</td>
<td>Management</td>
<td>5</td>
</tr>
<tr>
<td>PS</td>
<td>Personnel Security</td>
<td>Operational</td>
<td>8</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment</td>
<td>Management</td>
<td>4(5)</td>
</tr>
<tr>
<td>SA</td>
<td>System and Services Acquisition</td>
<td>Management</td>
<td>12(7)</td>
</tr>
<tr>
<td>SC</td>
<td>System and Communications Protection</td>
<td>Technical</td>
<td>24(16)</td>
</tr>
<tr>
<td>SI</td>
<td>System and Information Integrity</td>
<td>Operational</td>
<td>12(9)</td>
</tr>
</tbody>
</table>

*The number in parentheses in the last column includes the control enhancements required by the FedRAMP Moderate Baseline

For Cloud Service Providers, deploying and maintaining an infrastructure that meets the requirements established in the NIST and FedRAMP baseline requires centralized management and control of all components including virtual applications, platforms, and network devices.

The Federal Risk Authorization Management Program (FedRAMP) specifically began providing formalized guidance for cloud and virtual environments in June, 2012. These guidelines were based on industry feedback, rapid adoption of virtualization technology, and the move to cloud.
Figure 2: Official guidance on security in FedRAMP Cloud environments

NIST 800-53

The objective of NIST Special Publication 800-53 is to provide a set of security controls that can satisfy the breadth and depth of security requirements levied on information systems and organizations and that is consistent with and complementary to other established information security standards.

The catalog of security controls provided in Special Publication 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. It is the responsibility of organizations to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying their stated security requirements. The security controls in the catalog facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent and repeatable manner—thus contributing to the organization’s confidence that there is ongoing compliance with its stated security requirements.

The NIST 800-53 presents the fundamental concepts associated with security control selection and specification including: (i) the structure of security controls and the organization of the controls in the control catalog; (ii) security control baselines; (iii) the identification and use of common security controls; (iv) security controls in external environments; (v) security control assurance; and (vi) future revisions to the security controls, the control catalog, and baseline controls. Security controls described in this publication have a well-defined organization and structure. For ease of use in the security control selection and specification process, controls are organized into eighteen families. Each security control family contains security controls related to the security functionality of the family. In addition, there are three general classes of security controls: management, operational, and technical.

FedRAMP

Cloud computing technology allows the Federal Government to address demand from citizens for better, faster services and to save resources, consolidate services, and improve security. The essential characteristics of cloud computing—on-demand provisioning, resource pooling, elasticity, network access, and measured services—provide the capabilities for agencies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services.

Agencies have realized the benefits of this technology and are integrating it into their information technology environment. On December 9, 2010; the Office of Management and Budget (OMB) released the 25 Point Implementation Plan to Reform Federal Information Technology Management, establishing the Cloud First policy and requiring agencies to use cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. The Federal Risk and Authorization
Management Program (FedRAMP) was established by a memorandum issued by OMB on December 8, 2011, Security Authorization of Information Systems in Cloud Computing Environments (FedRAMP Policy Memo) to provide a cost-effective, risk-based approach for the adoption and use of cloud services. A key element to successful implementation of cloud computing is a security program that addresses the specific characteristics of cloud computing and provides the level of security commensurate with specific needs to protect government information. Effective security management must be based on risk management and not only on compliance. By adhering to a standardized set of processes, procedures, and controls, agencies can identify and assess risks and develop strategies to mitigate them.

The purpose of FedRAMP is to:

- Ensure that cloud based services have adequate information security;
- Eliminate duplication of effort and reduce risk management costs; and
- Enable rapid and cost-effective procurement of information systems/services for Federal agencies

FedRAMP was developed in collaboration with the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), the Department of Defense (DOD), and the Department of Homeland Security (DHS). Many other government agencies and working groups participated in reviewing and standardizing the controls, policies and procedures. The major participants in the FedRAMP process are:

- Federal agency customer – has a requirement for cloud technology that will be deployed into its security environment and is responsible for ensuring FedRAMP compliance
- Cloud Service Provider (CSP) – is willing and able to fulfill agency requirements and to meet security requirements
- Joint Authorization Board (JAB) – reviews the security package submitted by the CSP and grants a provisional Authority to Operate (ATO)
- 3rd Party Assessor Organization (3PAO) – validates and attests to the quality and compliance of the CSP provided security package
- FedRAMP Program Management Office (PMO) – manages the process assessment, authorization, and continuous monitoring process

A CSP follows the process for a provisional authorization under FedRAMP and uses a 3PAO to assess and review its security control implementations. CSPs then provide documentation of the test results in a completed assessment package to the FedRAMP PMO. The security package is then reviewed by the JAB and if a CSP system presents an acceptable level of risk, a provisional Authorization is granted. Agencies can then leverage the Provisional ATO and grant their own ATO without conducting duplicative assessments.

FedRAMP Continuous Monitoring Strategy & Guide

FedRAMP assessment process requires that monitoring activities be conducted continuously, quarterly, annually, every three years and every five years. These activities include required activities from the CSP and required activities of a 3PAO. The continuous monitoring program under FedRAMP is designed to provide more transparency into the ongoing security posture of the authorized cloud environment or service environment is acceptable.

The OMB memorandum M-10-15, issued on April 21, 2010, changed from static point-in-time security authorization processes to Ongoing Assessment and Authorization throughout the system development life cycle. Consistent with this new direction favored by OMB and supported in NIST guidelines, FedRAMP has developed an ongoing assessment and authorization program “Continuous Monitoring Strategy & Guide” for the purpose of reauthorizing Cloud Service Providers (CSP) annually. Traditionally, this process has been referred to as “Continuous Monitoring” as noted in NIST SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations. Other NIST documents such as NIST SP 800-37, Revision 1 refer to “ongoing assessment of security controls”. It is important to note that both the terms “Continuous Monitoring” and “Ongoing Security Assessments” mean essentially the same thing and should be interpreted as such.
Monitoring security controls is part of the overall risk management framework for information security and is a requirement for CSPs to maintain their FedRAMP Provisional Authorization. After a system receives a FedRAMP Provisional Authorization, it is possible that the security posture of the system could change over time due to changes in the hardware or software on the cloud service offering, or also due to the discovery and provocation of new exploits. Performing ongoing security assessments determines whether the set of deployed security controls in an information system remains effective in light of new exploits and attacks, and planned and unplanned changes that occur in the system and its environment over time. Ongoing assessment and authorization provides federal agencies using cloud services a method of detecting changes to the security posture of a system for the purpose of making risk-based decisions. Ongoing due diligence and review of security controls enables the security authorization package to remain current which allows agencies to make informed risk management decisions as they use cloud services. To receive reauthorization of a FedRAMP Provisional Authorization from year to year, CSPs must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable.

FedRAMP Continuous Monitoring Strategy & Guide is intended to provide CSPs with guidance and instructions on how to implement their continuous monitoring program. Certain deliverables and artifacts related to continuous monitoring that FedRAMP requires from CSP’s are discussed in this document.
CLOUD COMPUTING

Cloud computing and virtualization have continued to grow significantly every year. There is a rush to move applications and even whole datacenters to the “cloud”, although few people can succinctly define the term “cloud computing.” There are a variety of different frameworks available to define the cloud, and their definitions are important as they serve as the basis for making business, security, and audit determinations. VMware defines cloud or utility computing as the following (http://www.Vmware.com/solutions/cloud-computing/public-cloud/faqs.html):

“Cloud computing is an approach to computing that leverages the efficient pooling of on-demand, self-managed virtual infrastructure, consumed as a service. Sometimes known as utility computing, clouds provide a set of typically virtualized computers which can provide users with the ability to start and stop servers or use compute cycles only when needed, often paying only upon usage.”

Figure 3: Cloud Computing

There are commonly accepted definitions for the cloud computing deployment models and there are several generally accepted service models. These definitions are listed below:

- **Private Cloud** – The cloud infrastructure is operated solely for an organization and may be managed by the organization or a third party. The cloud infrastructure may be on premise or off-premise.
- **Public Cloud** – The cloud infrastructure is made available to the general public or to a large industry group and is owned by an organization that sells cloud services.
- **Hybrid Cloud** – The cloud infrastructure is a composition of two or more clouds (private and public) that remain unique entities, but are bound together by standardized technology. This enables data and application
portability; for example, cloud bursting for load balancing between clouds. With a hybrid cloud, an organization gets the best of both worlds, gaining the ability to burst into the public cloud when needed while maintaining critical assets on premise.

- Community Cloud – The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (for example, mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise.

To learn more about VMware’s approach to cloud computing, review the following:

- VMware Cloud Computing Overview
- VMware vCloud Architecture Toolkit

When an organization is considering the potential impact of cloud computing to its highly regulated and critical applications, it may want to start by asking:

- Is the architecture a true cloud environment (does it meet the definition of cloud)?
- What service model is used for the FedRAMP data environment (SaaS, PaaS, and IaaS)?
- What deployment model will be adopted?
- Is the cloud platform a trusted platform?

The last point is critical when considering moving highly regulated applications to a cloud platform. FedRAMP does not endorse or prohibit any specific service and deployment model. The appropriate choice of service and deployment models should be driven by customer requirements, and the customer’s choice should include a cloud solution that is implemented using a trusted platform.

VMware is the market leader in virtualization, the key enabling technology for cloud computing. VMware’s vCloud Suite 5.5 is the trusted cloud platform that customers use to realize the many benefits of cloud computing including safely deploying business critical applications. HyTrust enables the VMware compliance infrastructure by cumulatively addressing a larger set of controls across the NIST 800-53 Rev3 spectrum.

If you are an organization or partner that is interested in more information on the HyTrust Compliance Program, please email us at sales@hytrust.com.
WHERE TO START – CONSIDERATIONS FOR SYSTEM OWNERS, IT AND ASSESSORS

Migrating a traditional IT infrastructure to a virtual or cloud environment has a significant impact on an organization that extends beyond information technology. Security and compliance continue to remain top concerns for management, IT departments, and auditors. All three areas should be represented and engaged for any IT virtualization or cloud projects to confirm that business, IT operations, and compliance teams carefully consider the benefits and risks.

The following questions may be important when considering the potential business impact, benefits, and risks of a virtual and/or cloud environment.

IT Considerations
1. How does the IT Operations plan address the company’s strategic and operational goals?
2. What manual processes are in place that can be automated?
3. What are the skills and capabilities of the IT Department?
4. Have there been any previous attempts to virtualize or outsource critical operations?
5. Which IT initiatives currently underway could impact the FedRAMP system boundary?
6. How is encryption currently used to limit risk?
7. How is sensitive data currently classified (i.e., do you know where all your data resides)?
8. How has security and compliance affected IT Operations?

Assessment Considerations
1. What prior experience does the auditor have with virtual/cloud environments (Third Party Assessment Organization (3PAO))?
2. Has the 3PAO successfully assessed FedRAMP environments?
3. What certifications do they have in HyTrust products or solutions?
4. How many individuals that are part of the assessment team have experience with HyTrust?
5. What thought leadership and guidance has the 3PAO published?
6. What are the risks and mitigation techniques the 3PAO believes are appropriate for FedRAMP environments?
7. How long have they been working with HyTrust Solutions?
8. What references do they have for conducting similar assessments?
9. Is the 3PAO assigned to the audit engagement company knowledgeable about the basic components, systems, and software in a VMware cloud?
GUIDANCE FROM THE FEDERAL RISK AUTHORIZATION MANAGEMENT PROGRAM

HyTrust has identified the FedRAMP controls that highlight some of the critical requirements/guidance that organizations are required to address as part of their deployments. HyTrust has also provided information regarding how HyTrust tools are designed to help organizations address these controls.

Cloud computing technology allows the Federal Government to address demand from citizens for better, faster services and to save resources, consolidate services, and improve security. The essential characteristics of cloud computing -- on-demand provisioning, resource pooling, elasticity, network access, and measured services -- provide the capabilities for agencies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services.

Agencies can then leverage the Provisional ATO and grant their own ATO without conducting duplicative assessments. In prior cloud FISMA compliance projects, certain controls have proven to be challenging for service providers to meet. Before you decide to initiate a request to participate in FedRAMP, go through the below and make sure that you are truly able to meet these requirements. Consult with your legal team and technical staff (e.g. systems administrators, database administrators, network engineers etc.) to determine if you have the right controls in place and have the ability to manage them.

Checklist for CSPs getting ready to undergo the FedRAMP process

1. You have the ability to process electronic discovery and litigation holds
2. You have the ability to clearly define and describe your system boundaries
3. Review the Guide to Understanding FedRAMP
4. You can identify customer responsibilities and what they must do to implement controls
5. System provides identification & 2-factor authentication for network access to privileged accounts
6. System provides identification & 2-factor authentication for network access to non-privileged accounts
7. System provides identification & 2-factor authentication for local access to privileged accounts
8. You can perform code analysis scans for code written in-house (non-COTS products)
9. You have boundary protections with logical and physical isolation of assets
10. You have the ability to remediate high risk issues within 30 days, medium risk within 90 days
11. You can provide an inventory and configuration build standards for all devices
12. System has safeguards to prevent unauthorized information transfer via shared resources
13. Cryptographic safeguards preserve confidentiality and integrity of data during transmission
HYTRUST TECHNOLOGIES AND FEDRAMP

HyTrust products have been designed to help organizations support security and compliance needs. While every environment has unique needs, the following FedRAMP Compliance Stack provides a comprehensive mix of HyTrust solutions with features that are designed to assist with FedRAMP compliance. The solutions’ functionality, features, and specific NIST 800-53 Rev3 and FedRAMP Baseline Controls requirements are addressed in detail in the following sections.

Table 2: HyTrust Products

<table>
<thead>
<tr>
<th>SOLUTION AREA</th>
<th>KEY PRODUCTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>HyTrust</td>
<td>HyTrust CloudControl, HyTrust DataControl</td>
</tr>
</tbody>
</table>
HYTRUST FEDRAMP REQUIREMENTS MATRIX (OVERVIEW)

Coalfire has created a FedRAMP Requirements Matrix to assist organizations with an understanding of HyTrust, VMware and VMware Partner solutions (where they overlap), and the remaining customer responsibilities that must be addressed separately by the customer through use of other tools or processes. While every cloud is unique, HyTrust believes that a good portion of the technical controls listed in the NIST 800-53 Rev 3 and FedRAMP Baseline Controls requirements can be addressed through the VMware Suites and the HyTrust partner solutions. The controls addressed by HyTrust, VMware and the partners are primarily technical in nature and the remaining gaps in addressing FedRAMP requirements may be filled by the customer through other tools (i.e. approving customers’ policies, keeping an updated network diagram, approving changes, etc.)

HyTrust Boot Attestation Service with Intel TXT

A feature of the Intel® Xeon® processor, Intel TXT establishes a root of trust through measurements when the hardware and pre-launch software components are in a known good state. Utilizing the result, in combination with HyTrust CloudControl software, virtual infrastructure administrators can set policies for sensitive data and workload placements to occur only on trusted hypervisors and servers. This helps satisfy the FedRAMP requirement for Platform Integrity measurement and attestation, and for automated, policy-based Hypervisor Access Controls.

Intel TXT

Intel TXT validates platform trustworthiness during boot and launch, enabling reliable evaluation of the computing platform and its protection level. Intel TXT uses a Trusted Platform Module (TPM) and cryptographic techniques to provide “measurement” of software and platform components so that system software as well as local and remote management applications may use those measurements to make trust decisions. This technology defends against software-based attacks aimed at stealing sensitive information by corrupting system firmware or BIOS code, or modifying the platform’s configuration. Intel TXT verifies the integrity of platform components during boot and launch, including BIOS, operating system loader, and hypervisor.

Intel TXT provides strong signature-based integrity controls for individual systems and compute pools. The technology provides a signature that represents the state of an intact system’s launch environment. The corresponding signature at the time of future launches can then be compared against that known-good state to verify a trusted software launch, to execute system software, and to ensure that cloud infrastructure as a service (IaaS) has not been tampered with. Security policies based on a trusted platform or pool status can then be set to restrict (or allow) the deployment or redeployment of virtual machines (VMs) and data to trusted platforms with known security profiles. Intel TXT enables a trust model of a known software environment, that can be used to automatically verify systems and application integrity and ensures that the software being executed hasn’t been compromised. This advances security to give cloud service providers more than just detection-based security solutions. It also addresses key attack vectors.
**FEDRAMP REQUIREMENTS MATRIX (BY HYTRUST PRODUCT)**

**HyTrust CloudControl**

HyTrust CloudControl provides access control, visibility and secure multi-tenancy to virtual infrastructure. Critical security functionality that it provides includes strong authentication and root password vaulting, granular administrative policies and audit-quality logging and alerting. These are key features that Cloud Service Providers need to meet in order to provide sound compliance solutions for FedRAMP.

**Figure 4: HyTrust Cloud Control**

![HyTrust Cloud Control Diagram]

The following product matrix explains which FedRAMP controls are applicable to the HyTrust Infrastructure. It specifically explains how HyTrust CloudControl enables users to meet FedRAMP requirements.
### Table 2: Applicability of FedRAMP Controls to HyTrust CloudControl

<table>
<thead>
<tr>
<th>NIST 800-53 Control Family</th>
<th>Controls Address</th>
<th>HyTrust CloudControl Applicability Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS CONTROL</td>
<td>AC-2, AC-3(3), AC-4, AC-5, AC-6, AC-6(2), AC-10</td>
<td>HyTrust enables cloud service providers to fully manage access to the cloud infrastructure. As a centralized security gateway, all actions are tied to the identity of the specific user. Role based access control policies can be implemented to ensure authorized personnel only have access to systems and functions that they are assigned to. Granular auditing provides monitoring and enforcement of access policies. HyTrust supports two-factor authentication which is a requirement under FedRAMP for administrative and remote access to cloud environments. Root Password Vaulting securely stores root passwords and in the event access is required at that level a one-time access password is generated and logged for specified administrators. In addition to the creation of organizational policies and procedures to enforce access through approved authorizations only, there needs to be technical configurations to enforce these policies and procedures. Through the implementation of role based access controls and identity binding, HyTrust ensures access to the cloud environment and infrastructure is restricted only to personnel with approved authorizations. Through the implementation of role based access controls and identity binding HyTrust ensures access to the cloud environment and infrastructure is restricted to personnel with approved authorization. Access authorizations can be defined and automatically enforced across the entire virtual infrastructure using policy templates enabling organizations to implement effective separation of duties and least privilege across the cloud service boundary. In cases where changes are made to resources and virtual environments, secondary approval is required before the change can be committed. Using the HyTrust product suite, cloud service providers can develop and implement security templates to enforce least privilege for access rights tailored to role or assigned tasks. HyTrust CloudControl actively monitors and enforces policy driven access control settings and policies across all managed assets within the cloud service. HyTrust integrates with Active Directory and LDAP to ensure only organizationally authorized privileged accounts can perform security functions or access security relevant information within the cloud management layer and infrastructure. Fine-grained authorization features built-in to the HyTrust CloudControl system allows organizations to configure and enforce least privilege based on roles and assets, preventing non-privileged or unauthorized accounts from accessing security functions or security relevant information across the entire virtual infrastructure. Security Templates can be tailored to meet FISMA and FedRAMP policy requirements limiting the number of concurrent sessions for privileged and non-privileged access to devices and assets across the virtual infrastructure.</td>
</tr>
<tr>
<td>AUDIT AND ACCOUNTABILITY</td>
<td>AU-2, AU-3, AU-6, AU-8(1), AU-12</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HyTrust CloudControl provides forensic level logging functionality that centrally records every action attempted by every vSphere user of every tenant conducted through any management interface. HyTrust logs contain considerably more detail than platform logs, including source IP addresses and records of failed and denied attempts. Most importantly combined with the security policy templates, HyTrust CloudControl establishes an audit trail by tying every record to the unique ID of the user who attempted the operation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A key feature within the HyTrust is the ability to provide fine-grained auditing. HyTrust CloudControl provides the ability to log a broad range of activities including the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Logging of all administrative actions across the virtual infrastructure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Modification of account roles and privileges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Security, access and audit policy creation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Creation and deletion of virtual machines</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Modification of virtual machine privileges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VM access from storage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Back-up image generation and restoration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HyTrust CloudControl can automatically send audit records to SIEMs and other security monitoring and management systems such as McAfee ePolicy Orchestrator, McAfee ESM, VMware Log Insight, Symantec Control Compliance Suite, RSA enVision and HP ArcSight. This allows cloud service providers to actively monitor and report on audit events of interest across their management and service infrastructure and tenant VM's.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Timestamps are generated by the HyTrust platform and from the VMware ESXi systems managed by the appliance. Interoperability with Microsoft Active Directory allows an additional organizationally defined authoritative time source, for cloud service providers who need to implement primary and secondary time services. Multiple NTP server IP addresses can be added in a comma separated list within the management console of the appliance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HyTrust audit logs generally contain a date and timestamp, hostname, priority, a message ID, and additional information to support after-the-fact investigations. The granularity of audit records generated by the HyTrust system allows security personnel to determine who performed an action, what time and from what location, and to what target object.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SECURITY ASSESSMENT AND AUTHORIZATION</th>
<th>CA-7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HyTrust allows cloud service providers the ability to actively monitor and report on security and policy related events. Organizations required to maintain a continuous monitoring capability can leverage the monitoring and reporting capabilities built-in to the HyTrust platforms for assessing the security status of their cloud infrastructure and tenant VM’s. Interoperability with SIEMS and other security monitoring platforms allows organizations to correlate audit logs across all of their devices and assets.</td>
</tr>
</tbody>
</table>
| **CONFIGURATION MANAGEMENT** | CM-2, CM-3, CM-5, CM-6, CM-9(3) | Security compliance templates can be developed and configured across all managed hosts within the virtual infrastructure. Organizations seeking FedRAMP compliance can monitor configuration of assets using CIS benchmarks, VMware recommended security hardening settings or customized compliance settings. Configuration changes can be audited by the HyTrust appliance to ensure active monitoring to enforce configuration control across virtual devices and assets within the cloud infrastructure.

HyTrust CloudControl provides key configuration hardening capabilities to VMware’s ESX or ESXi Hypervisor. Configuration policies can be defined and automatically deployed to ensure hardening requirements are consistently implemented. HyTrust also provides active monitoring and automatic remediation of any unauthorized configuration changes.

Logging and alerting on configuration changes made to assets and virtual devices is a key capability provided by the HyTrust product suite. Granularity of auditable events and the ability to import predefined hardening checklists or organization defined checklists, allows for greater control and oversight of configuration changes across the entire cloud service infrastructure.

Role and asset based access controls can be configured in HyTrust, providing cloud service organizations an automated capability for monitoring and enforcing access control requirements. HyTrust’s auditing and monitoring capabilities provides additional enforcement features to ensure logical access restrictions are consistently applied across the entire infrastructure.

Security policy and configuration checklists and benchmarks are incorporated into HyTrust and these can be used to monitor and enforce approved configuration settings. Organizations can actively monitor and prevent unauthorized changes to the configuration settings of virtual assets and devices.

Used in combination with Intel TXT, organizations can automatically monitor and detect unauthorized software and firmware components in real time. Remediation actions can be automatically employed, or manually applied upon alerting and investigation by security or systems personnel. |
| **IDENTIFICATION AND AUTHENTICATION** | IA-2 (11), IA-5, IA-5(1) | HyTrust provides strong multifactor authentication capabilities, including integration with RSA SecurID. By managing access authorizations and authentication methods through the HyTrust appliance, cloud service providers can apply multifactor authentication across their entire virtual infrastructure without having to make any manual changes to tenant VM's or other managed devices or hosts.

HyTrust binds the identity of access accounts to assigned personnel, enabling organizations to provide account and authenticator management oversight. Additional functionality within the HyTrust product suite can be enabled to provide organizations effective control of passwords and password strength. Cloud service providers can use HyTrust to remove and replace default passwords, in addition to managing appropriate password strength for access accounts. Root Password Vaulting is an additional feature that allows HyTrust to automatically manage individual hosts managed by root accounts. Using the Root Password Vaulting feature, the HyTrust appliance will create a new secure root password on the selected host, and store it in a password vault. HyTrust will automatically rotate or update the root password on a regular basis, in keeping with authenticator expiration timeframes required by NIST and FedRAMP required frequencies. |
HyTrust allows security administrators to establish and enforce password complexity rules on the HyTrust appliance as well as defining password rules on managed hosts within the virtual environment. One-time root passwords can be issued to authorized administrators to access root functions on managed hosts.

| SYSTEM AND COMMUNICATIONS PROTECTION | SC-5, SC-10 | HyTrust provides hardening and protection capabilities for the hypervisor and critical virtual assets within the cloud infrastructure, in order to protect against malicious or accidental corruption and denial of service to customers within large multi-tenant environments.

Platform Integrity w/ Intel TXT and hypervisor access control by protocol and IP allows organizations to monitor remote connections and enforce automated disconnect settings. |

| SYSTEM AND INFORMATION INTEGRITY | SI-3, SI-7 | The use of security templates by HyTrust to manage approved configurations and access control settings, allows organizations to monitor and automatically alert/remediate upon discovery of unauthorized changes to virtual assets and privileges which could be caused by malicious code. The fine-grain auditing and logging features allow security personnel to determine source and extent of infection in the event of malicious code being active within the cloud service infrastructure.

Used in combination with Intel TXT, any unauthorized code or changes across physical platforms and devices can be detected immediately enabling the administrator to quarantine the affected systems.

HyTrust provides integrity protection and verification capabilities across assets and devices within the cloud infrastructure. HyTrust CloudControl secures and monitors configuration settings of virtual assets and critical components/devices. Unauthorized changes are detected and reported by the HyTrust appliance, which can also automatically remediate the change in configuration. |
HyTrust DataControl

HyTrust DataControl locks down critical applications and data with strong encryption and centralized key control. These features allow Cloud Service Providers and their respective customers to lock down applications and data before deploying to a public cloud. Customers are able to generate an encryption key that they can manage, preventing even the Cloud Service Provider from accessing their data.

HyTrust KeyControl is an integral part of the DataControl suite. KeyControl is a locked-down appliance that can be easily deployed on physical or virtual servers. In tandem with the HyTrust DataControl encryption engine, KeyControl provides automated, centrally managed control over all encryption and key management policies.

Figure 5: HyTrust Data Control

The following product matrix explains which FedRAMP controls are applicable specifically to HyTrust DataControl. It also explains how the DataControl product assists users in meeting FedRAMP requirements.
### Table 3: Applicability of FedRAMP Controls to HyTrust DataControl

<table>
<thead>
<tr>
<th>NIST 800-53 R3 AND FEDRAMP BASELINE CONTROLS</th>
<th>HYTRUST DATACONTROL APPLICABILITY DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYSTEM AND COMMUNICATION PROTECTION</strong></td>
<td></td>
</tr>
<tr>
<td>SC-12, SC-28</td>
<td>HyTrust KeyControl provides strong authentication and key management capabilities to ensure that only authorized personnel or devices have access to the key management functions and decryption keys used to encrypt workloads through the DataControl software. HyTrust DataControl encrypts customer data and assigns encryption keys to the data owner, in order to protect against unauthorized access or modification or customer data. FIPS validated encryption is used to ensure the integrity of data is maintained according to FedRAMP requirements for security of sensitive information. HyTrust DataControl has the ability to detect the presence of the Intel® Advanced Encryption Standard New Instructions (AES-NI); which is a specialized instruction set for the Intel Xeon and Core processor families that enables faster and more efficient encryption using the AES algorithm.</td>
</tr>
</tbody>
</table>
Disclaimer:

* HyTrust solutions are designed to help organizations address various regulatory compliance requirements. This document is intended to provide general guidance for organizations that are considering HyTrust solutions to help them address such requirements. HyTrust encourages any organization that is considering HyTrust solutions to engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements. It is the responsibility of each organization to determine what is required to meet any and all requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide legal advice and is provided “AS IS”. HyTrust makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Nothing that you read in this document should be used as a substitute for the advice of competent legal counsel.

Acknowledgements:

HyTrust would like to recognize the efforts of the VMware Center for Policy & Compliance, VMware Partner Alliance, and the numerous teams that contributed to this paper and to the establishment of the HyTrust Compliance Program. HyTrust would also like to recognize the Coalfire Systems Inc. www.coalfire.com/Partners/HyTrust for their industry guidance. Coalfire®, a leading FedRAMP firm, provided FedRAMP guidance and control interpretation aligned to NIST 800-53 Rev3 and FedRAMP Baseline Controls and the Reference Architecture described herein.

The information provided by Coalfire Systems and contained in this document is for educational and informational purposes only. Coalfire Systems makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein.

About Coalfire

Coalfire Systems is a leading, independent information technology Governance, Risk and Compliance (IT GRC) firm that provides IT audit, risk assessment and compliance management solutions. Founded in 2001, Coalfire® has offices in Dallas, Denver, Los Angeles, New York, San Francisco, Seattle and Washington, D.C., and completes thousands of projects annually in retail, financial services, healthcare, government and utilities. Coalfire has developed a new generation of cloud-based IT GRC tools under the Navis® brand that clients use to efficiently manage IT controls and keep pace with rapidly changing regulations and best practices. Coalfire’s solutions are adapted to requirements under emerging data privacy legislation, the NIST 800-53 Rev3 and FedRAMP Baseline Controls, GLBA, FFIEC, HIPAA/HITECH, NERC CIP, Sarbanes-Oxley and FISMA. For more information, visit www.coalfire.com.