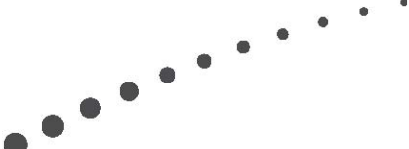




Citrix Cloud Solution for Compliance





Contents

Introduction.....	3
Fitting Compliance to the Cloud	3
Considerations for Compliance in the Cloud	4
Citrix Cloud Solution for Compliance.....	7
Summary	12
Additional resources.....	12

INTRODUCTION

Enterprises today face increasing challenges meeting the various compliance and regulatory requirements applicable to them. This burden is significantly increased if the enterprise has operations in various geographies or across different verticals. For instance, an e-commerce vendor with global customers needs to comply with data privacy and disclosure mandates such as the EU Data protection directive, California privacy laws and PCI-DSS. Moreover, as a response to the recent economic crises, more regulatory and compliance mandates are expected as governments and regulatory bodies shore up requirements in an attempt to prevent future incidents.

Instead of treating each compliance requirement as an independent, siloed effort, an organization can achieve significant reductions in effort and cost by adopting standards such as ISO27002 as the base security guidance. In addition, a Governance, Risk and Compliance (GRC) framework allows the organization to avoid conflict, reduce overlap and gaps and gives better executive visibility to the risks faced. It also enables the organization to be proactive in addressing risk and compliance issues.

FITTING COMPLIANCE TO THE CLOUD

Cloud computing offers a new way of delivering computing resources instantly, on-demand and inexpensively. The reduced cost and flexibility of cloud-based services is attractive to organizations of all sizes from SME's to large enterprises. Governments are also interested in using cloud computing to reduce IT costs and increase capabilities. Meeting compliance requirements by moving to a cloud-based solution offers significant benefits.

Improved compliance. The chief benefit most cite for cloud computing is either increased flexibility or lower costs. However, given the complexity of meeting today's compliance mandates, the biggest benefit may be better compliance. Most compliance and regulatory requirements deal with data and process security and control.

A centralized, cloud-based solution can, due to significant economies of scale, provide a more secure infrastructure than a one-off approach effort. This can range from physically hardened datacenters to better and resilient network connectivity and security threat protection as well as a dedicated Incident Response (IR) team that can help diagnose and quickly respond to any issues that arise.

Lower costs. A cloud-based compliance solution can potentially reduce costs in two key ways. First, the economies of scale discussed earlier can make using a cloud-based solution cheaper than building out and maintaining a completely private compliance infrastructure. Second, using the cloud changes a capital expense to an operational expense, which for certain companies and industries has significant financial benefits.



Capacity on demand. Compliance, or the lack thereof in the cloud, is often cited as a barrier to cloud adoption. A lack of compliance services in the cloud makes tapping the elasticity of the cloud impossible for workloads that must meet compliance mandates. However, a cloud-based solution that incorporates compliance services opens up the general benefits of the cloud to many more applications.

CONSIDERATIONS FOR COMPLIANCE IN THE CLOUD

Depending upon business process (e.g., processing credit card transactions) or industry (e.g., healthcare) most organizations are subject to various compliance and regulatory mandates. For example, publicly traded financial services institutions located in the United States operating their own datacenters where both customer and corporate data and applications are located must comply with:

- Graham-Leach-Bliley Act (GLBA) /FFIEC guidelines
- Payment Card Industry (PCI)
- SAS-70 Type-II audits
- Various state and federal privacy and data breach disclosure requirements

Some of the common compliance standards are listed in the following table:

Industry Vertical / Geo	Compliance standard
Financial – US	FISMA, GLBA, PCI-DSS
Utility – US	NERC, FERC, State regulations
Healthcare – US	HIPAA, HITECH
Data privacy – various	EU data directive, SB-1386 (CA), Canada – PIPEDA, Aus, NZ privacy acts
Public Companies	SOX, J-SOX
Government	FISMA, NIST controls

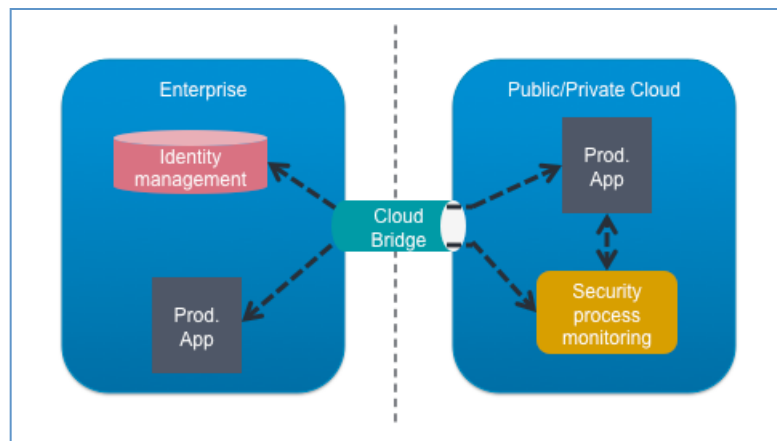
To demonstrate compliance to auditors and regulators, firms rely upon reporting and auditing frameworks that map compliance requirements to specific controls and policies that have been implemented.

Moving core IT services to the cloud does add challenges to meeting the compliance mandate. Some control of certain aspects of the service (the infrastructure, data, provisioning etc) is ceded to the cloud provider, though exactly how this is manifested depends upon how the cloud solution is implemented. Regardless, the cloud solution must provide the same types of safeguards and controls that are otherwise implemented privately. The cloud provider must also be able to provide evidence of compliance by providing regulation-specific reports and audits such as SAS-70 reports.

Once it is established that a cloud solution meets the necessary compliance mandates, migrating an application to the cloud, or rolling out a new application service within the cloud requires:

1. A secure bridge and access between cloud and enterprise data center

A secure bridge needs to be maintained between the cloud data center and the enterprise. This provides seamless, secure connectivity and enables certain security services (e.g., compliance reporting) running in the cloud to be used with applications running within the enterprise datacenter. This also allows the identity management infrastructure (e.g., directory services) running in the enterprise to be leveraged by applications running in the cloud.



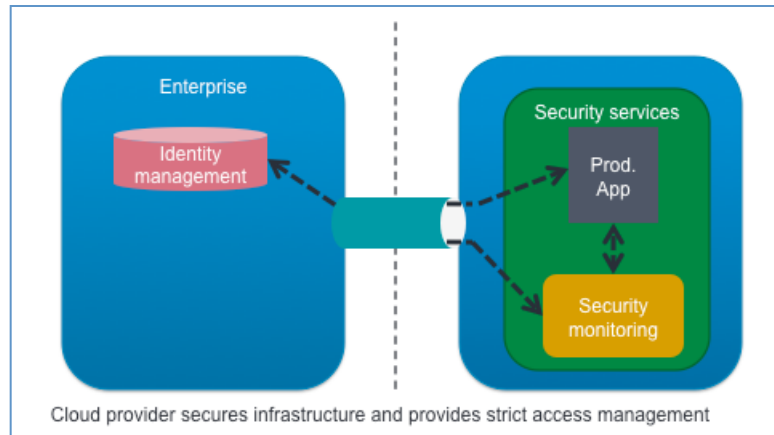
2. Onboarding applications into physically secure datacenters

Moving an application into a cloud data center can be complex, even if compliance issues are put aside. The application itself likely consists of far more components than will initially appear, and some of these components, especially those like directory services that are shared by other applications, likely cannot be moved to the cloud. Conversion – be it physical-to-virtual (P2V) or virtual-to-virtual (V2V) – between how the application is hosted in the enterprise vs. how it will run within the cloud also must be considered. Onboarding services can simplify this migration process, reducing both cost and risk. Please see the Citrix Cloud Solution for Onboarding for a more detailed discussion.

In terms of the target cloud data center itself, most regulatory and compliance mandates require certain levels of physical security for the data center environments. For example, SAS-70 Type-II audits require that all access to the application servers and data is secure and that audit trails are maintained. Thus the target cloud data center must meet these compliance requirements.

3. Secure Networking

Almost all compliance mandates require network security, though some mandates (e.g., PCI-DSS) are far more proscriptive than others in defining exactly what will meet this requirement. A compliance solution will likely use a combination of network firewalling and VPNs, intrusion prevention and detection (IPS/IDS), load balancing and application firewalling to provide network security. In many cases, these services will be provided to protect both the entire cloud data center, and well as specifically to protect the enterprise workload running in the cloud.

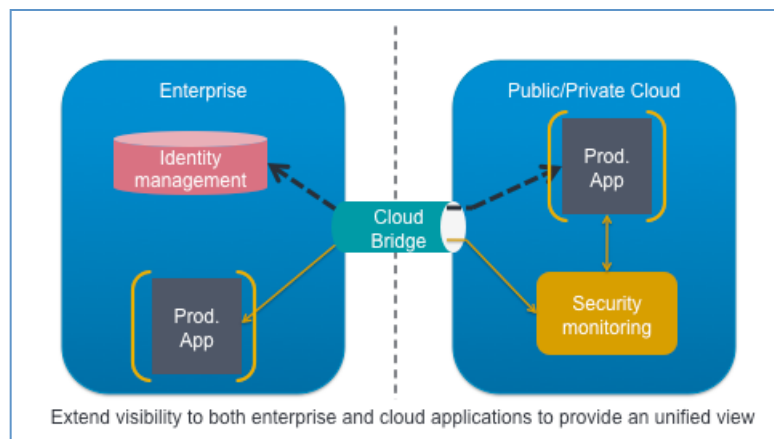


4. Security Monitoring

To assure the adequacy of their risk mitigation strategy and implementation, network and host activity must be monitored to identify policy violations, anomalous behavior, unauthorized configurations and other risky conditions. This can be done by log monitoring and SIEM tools (Security Incident and Event management) that can quickly identify, classify, escalate report and guide responses to security events.

5. Maintaining a Unified Cloud / Datacenter View

As the lines between one application and another continue to blur, certain components of an application may continue to execute in the enterprise data center even though the majority of the app may be hosted in the cloud. Or, the inverse can be true. In these cases, security and associated application management services running in the cloud should be extensible to cover components running in the enterprise data center (and vice versa). For example, security process monitoring services running in the cloud should be able to receive events from applications executing in the enterprise data center.





6. Security Process Monitoring and updating

Even though the application is executing off-premise, there is still the need to continuously gather and analyze new threats and vulnerabilities, respond to actual attacks and monitor the effectiveness of the existing security controls. Any new information and analysis should also result in updating the security, risk and implementation controls. This is distinct from Security monitoring as it focuses on whole security process and not current security events. This includes services like vulnerability scanning, and penetration testing as well as threat monitoring and analysis.

7. Establishing the Governance, Risk and Compliance (GRC) framework

Maintaining compliance involves coordinating across individual domains such as policy, threat, incident, audit, and business continuity management. A comprehensive compliance solution will provide largely turnkey integration of all these domains, and provide the enterprise visibility into their applications' status. This includes implementing an ongoing security process that

- Maintains a risk assessment program that monitors assets and data threats
- Prioritizes risk
- Develops a security strategy that defines control objectives
- Establishes an implementation plan.

CITRIX CLOUD SOLUTION FOR COMPLIANCE

Citrix Cloud Partners use a combination of their internally developed technology and processes coupled with infrastructure from Citrix and technology partners to meet these requirements.

Requirement	Citrix Cloud Solution Capability
Implementing an ongoing security process, a risk assessment program that monitors assets and data threats to prioritize risk and develops a security strategy that defines control objectives and establishes an implementation plan.	Governance, Risk and Compliance framework
Maps requirements in the applicable compliance standards (HIPAA, PCI etc) to specific controls and policies that have been implemented.	Standard specific reporting and audit modules
Gather and analyze new threats and vulnerabilities, actual attacks and monitor the effectiveness of the existing security controls.	Security process monitoring and updates

Monitor network and host activity to identify policy violations, anomalous behavior, unauthorized configurations and other risky conditions.	Security monitoring
Protection for data while it is at rest, in motion and in use.	Data Protection
Policy-driven control of orchestration, management and security for compute, network and storage resources	Open Cloud Framework
Ability to extend the identity management infrastructure across the enterprise and the cloud deployment.	Cloud Access Services
Seamlessly connect the enterprise datacenter and the cloud datacenter with full security, performance and network transparency	Cloud Bridging Services
Easily allocate pooled network, CPU and memory capacity to bring up server, application, and network appliance instances on demand.	Platform Virtualization
Ensure the performance, availability and security of network and server resources running within the cloud data center	Edge Networking Services
Physical hardened datacenter resilient against disasters and network security attacks with dedicated support and Incident Response.	Hardened Datacenter

Governance, Risk and Compliance Framework

Maintaining compliance requires total visibility of both past events and future trends. A governance, risk and compliance framework allows the organization to manage specific technical risks and how they affect governance and compliance. It also helps better manage ongoing compliance efforts by reducing duplication of effort and bringing it into the mainstream management process. The RSA Archer compliance portal provides a holistic view across organizational boundaries as well as a single compliance-oriented application.

For more information on how RSA Archer can help with a GRC framework, [click here](#).

Compliance standard-specific reporting and audit modules

Every organization may have specific compliance requirements based on geography or industry vertical. By tapping into data (e.g., logs, events) from the applications and various security



monitoring and enforcement points, custom reports that are mapped to specific regulations or standards like PCI-DSS, HIPAA, SOX, ISO27002 etc., can be used to demonstrate compliance and provide an audit trail for verification.

Some of the common compliance standards are listed in the following table:

Industry Vertical / Geo	Compliance standard
Financial – US	FISMA, GLBA, PCI-DSS
Utility – US	NERC, FERC, State regulations
Healthcare – US	HIPAA, HITECH
Data privacy – various	EU data directive, SB-1386 (CA), Canada – PIPEDA, Aus, NZ privacy acts
Public Companies	SOX, J-SOX
Government	FISMA, NIST controls

For more information on how ArcSight helps meet compliance reporting and audit needs, [click here](#).

Security process monitoring and updates

Compliance is reliant on a solid security foundation. Security must not only be designed in, it must be continually assessed and tested against both common and application-specific risks. For example, the ability to test version upgrades of a web application for technical security vulnerabilities and ensure that the upgrade is still in compliance with organizational policies and regulations is critical. Protection against specific threats such as the OWASP Top 10 and ensuring compliance with PCI DSS Requirement 6.5 needs to be tested and verified.

For more information on how Cenzeic Hailstorm can help meet this requirement, please [click here](#).

For more information on how Citrix® XenApp™ helps meet process monitoring requirements, please [click here](#).

Security monitoring

Critical to maintaining compliance, as well as other application service levels, is the ongoing monitoring of the application, the application's performance, and the larger security environment. Application visibility solutions provide full L4-7 visibility, enabling detailed insight into what information and data is flowing, as well as providing insight into application performance service levels. Security incident and event monitoring (SIEM) consolidates log data, indicates trends, provides alerts for required action items and provides detailed reporting capabilities for systems managers as well as foundational information for GRC tools. In addition to providing visibility into



the current security state, SIEM is also critical to proving compliance was maintained during previous reporting periods and for assessing whether planned modifications and enhancements maintain the appropriate compliance posture.

For more information on how CoRadiant provides application visibility to help ensure performance and compliance service levels, [click here](#).

For more information on how the ArcSight SIEM platform helps meet these requirements, [click here](#).

Data protection

Network security is critical to overall security. However, the Jericho Forum has stated that an over-reliance on perimeter security has resulted in today's security disasters. Application and desktop workloads in the cloud need to be protected from malware and compromise. The ultimate perimeter is highly specific to the needs of individual needs of sensitive data. The new perimeter must be around the data while it is at rest, in transit and in use.

For information on how Citrix XenApp and Citrix XenDesktop™ help meet data protection needs, [click here](#).

Open Cloud Framework

Cloud framework services provide the foundational logic for rapidly provisioning, managing and controlling workloads deployed into multi-tenant, shared infrastructure clouds. The cloud framework ensures policy enforcement and security, and provides for integration with existing services such as billing, metering and self-service portals. Interoperability with other popular Cloud interfaces, and extensibility of the framework itself, provide the flexibility to leverage existing investments when migrating between clouds.

For more information on how Citrix CloudController™ provides an extensible, full-featured policy engine for controlling a heterogeneous, multi-tenant environment, [click here](#).

Cloud Access Services

Citrix CloudAccess™ is a pragmatic solution to the cross-domain authentication problem that leverages existing enterprise infrastructure and works to extend the policy framework that has already been put in place. Features include: Unified Password Management for SaaS, SSO to Cloud/SaaS applications, Password Workflow Automation, support for all major SaaS providers, and integrates into the with full transparency. Benefits include: Improve security across all applications, no end user training required standardizes password policy across both internal and external applications, automatically removes access to applications for users removed from the enterprise authentication framework, and simplifies password reset for end users.

For more information on Citrix CloudAccess™, [click here](#).

Cloud Bridging Services

All but the simplest cloud use cases will require a secure, persistent connection between enterprise and cloud data centers. While this “bridge” does incorporate VPN services for security, the bridge is much more than a VPN tunnel. Strategically, the key role of the bridge is to provide an overlay network across physical and virtual topologies, making the cloud a seamless extension of the



enterprise network. With the cloud a transparent extension of the enterprise network, migrating application workloads becomes far easier since the applications network-specific configurations won't need to be overhauled.

For more information on Citrix CloudBridge™, which leverages key capabilities within Citrix NetScaler, Citrix XenServer and Citrix Branch Repeater, please [click here](#).

Edge Networking Services

Edge networking services are critical to ensuring the reliability, security and performance of any cloud-based offering. Properly deployed, these services are largely transparent to the cloud consumers, yet are fundamental to ensuring the cloud remains available in the face of natural and man-made disasters, hacker attacks, planned and unplanned network and server outages and unanticipated surges in traffic.

Citrix NetScaler® is an integrated Web application delivery controller that provides advanced traffic management through Layer 4-7 load balancing and content switching. Global server load balancing provides critical business continuity and disaster recovery support during site-level disruptions and outages. NetScaler also includes application security via a web application firewall and SSL VPN. *For more information on Citrix NetScaler, [click here](#).*

Citrix Branch Repeater™, available as a physical or virtual appliance, is a WAN optimization solution that provides a high definition desktop and application experience to branch and mobile users while dramatically reducing WAN bandwidth costs and simplifying branch infrastructure. Branch Repeater accelerates desktop and application delivery, decreases WAN bandwidth consumption, and enables server consolidation. *For more information on Citrix Branch Repeater, [click here](#).*

Platform Virtualization

Server, storage and network virtualization are linchpins of the flexibility, affordability and scalability of any cloud-based offering. By simultaneously optimizing resource utilization through consolidation while still maintaining full isolation, virtualization supports the cost effectiveness of cloud offerings. By abstracting workloads from the underlying physical resources that run them, virtualization enables the elasticity needed for cloud services to be made available on-demand and self-service.

Citrix XenServer™ is the only enterprise-class, cloud-proven server virtualization platform that delivers the critical features of live migration and centralized multi-server management at no cost. XenServer is an open and powerful server virtualization solution powered by the industry-standard Xen® hypervisor, and created by the inventors of Xen. *For more information on XenServer, [click here](#).*

Citrix NetScaler VPX™ provides complete NetScaler functionality in a simple, easy to install virtual appliance. With NetScaler VPX, load balancing and web application acceleration, security and offload are available as virtualized services anywhere within the cloud. *For more information on Citrix NetScaler VPX, [click here](#).*

SUMMARY

The Citrix Cloud Compliance Solution presents the best architecture for compliance. Utilizing a public or private service leverages the predefined controls, templates and workflow to ensure that compliance measures are always active and measurable and that requirements are defensibly met. A professionally managed and architected compliance service results in compliance being inherent in the delivered solution – and not bolted on after the fact. Applications and data subject to compliance regulations are delivered through the cloud service architecture and compliance rules are programmatically enforced.

The key benefits of the Compliance Solution are:

- Compliance is enforced from datacenter to cloud (public or private) for all in-scope applications and data, with no application modification.
- Controls such as strong authentication, access control, end-to-end encryption and advanced audit logging are immediately available and consistent across applications.
- Management and auditing are greatly facilitated through the use of centralized controls and deep integration of Citrix Ready partner solutions.
- The cloud provider can often provide security and compliance services in a cost effective manner due to larger economies of scale.

The Citrix Compliance solution integrates and manages the controls and workflow necessary to easily and cost-effectively achieve and maintain compliance for any type of application architecture.

ADDITIONAL RESOURCES

To learn more about the Terremark Enterprise Cloud, and how it provides end-to-end compliance, please [click here](#).

FFIEC Information Security IT Examination handbook,
http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

Cloud Computing - Benefits, Risks and recommendations for information security: European Network and Information Security Agency (ENISA), Nov 2009.
<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>



About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is the leading provider of virtualization, networking and software as a service technologies for more than 230,000 organizations worldwide. Its Citrix Delivery Center, Citrix Cloud Center (C3) and Citrix Online Services product families radically simplify computing for millions of users, delivering applications as an on-demand service to any user, in any location on any device. Citrix customers include the world's largest Internet companies, 99 percent of Fortune Global 500 enterprises, and hundreds of thousands of small businesses and prosumers worldwide. Citrix partners with over 10,000 companies worldwide in more than 100 countries. Founded in 1989, annual revenue in 2008 was \$1.6 billion.

©2010 Citrix Systems, Inc. All rights reserved. Citrix®, Access Gateway™, Branch Repeater™, Citrix Repeater™, HDX™, XenServer™, XenApp™, XenDesktop™ and Citrix Delivery Center™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.