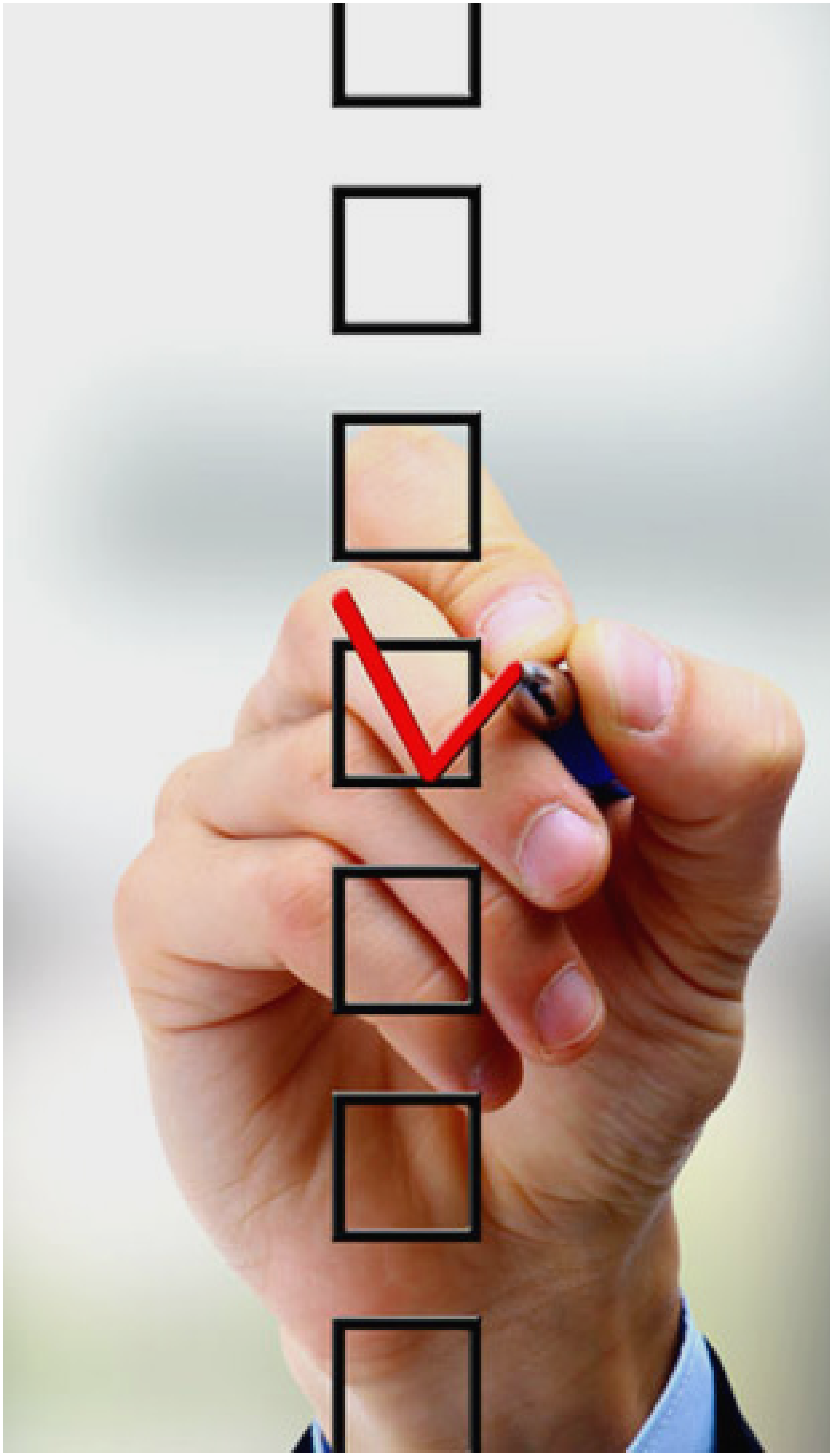
RapidScale

White Paper

Compliance in the Cloud

Compliance in the Cloud

Compliance, in terms of business, refers to the laws and regulations that organizations must abide by as they conduct business in their respective industry. It is something that every business should be familiar with. RapidScale recognizes the importance of these rules and has established its data encryption, protocols and procedures to follow the top compliances and ensure that customer data remains secure and confidential.



Some of the largest compliance laws include HIPAA, PCI DSS and Sarbanes-Oxley. Whether or not these individual regulations pertain to your organization, it's important to be aware of them so issues don't sneak up on you. If you're storing confidential information but don't have compliance expertise, you run the risks of device theft, unauthorized access to that confidential data, loss of files, and hacking or IT incidents.

The cloud can help. 94% of businesses reported that they saw an improvement in security after switching to the cloud. Organizations are moving to the cloud to ensure that their data is protected and encrypted. RapidScale is a leader in this transition.

A common misconception about compliance is that if your cloud provider is compliant, you are too. Unfortunately this is not the case, and it is a misconception that can lead to fines and even a halt of business operations. There is responsibility on both ends when it comes to compliance, and when it comes down to it, the data owner is ultimately responsible for protecting the data. The organization should monitor the provider's compliance for applicable requirements, while the provider should be able to provide ongoing assurance that the requirements are being met. It's important to have that conversation with the cloud provider - typically you can work together to allocate responsibility regarding security and compliance.

Common Regulations

HIPAA

The Health Insurance Portability and Accountability Act, commonly known as HIPAA, is intended to improve the efficiency and effectiveness of the health care system. It requires the adoption of national standards for electronic health care transactions and code sets, as well as unique health identifiers for providers, health insurance plans and employers. The law recognizes that electronic technology could erode the privacy of health information and incorporates provisions for guarding the security and privacy of personal health information. It enforces national standards to protect individually identifiable health information (known as the Privacy Rule) and the confidentiality, integrity and availability of electronic protected health information (known as the Security Rule).

PCI DSS

PCI DSS is a set of requirements for enhancing the security of payment customer account data. This standard was developed to help facilitate global adoption of consistent data security measures. It includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. It is essential for all businesses that accept credit cards, whether online or offline, to ensure that the payment card data remains secure. While the size of the organization determines the specific requirements that must be met, PCI DSS applies to both huge corporations and small online businesses.

SOX Act

The Sarbanes-Oxley Act, or SOX, is designed to protect investors and the general public by increasing the accuracy and reliability of corporate disclosures. SOX is administered by the Securities and Exchange Commission, which publishes SOX rules and requirements defining audit requirements and the records businesses should store and for how long. SOX is organized into 11 titles to protect against accounting errors and fraudulent practices in business.

What to Look For From a Cloud Provider

Today, the benefits of cloud computing are widely recognized, and that means that providers have been forced to pay more attention to compliance and helping customers achieve it. Therefore, processes in this area are improving. When an organization looks to move data to the cloud, but also needs to meet compliance regulations, it does take a bit of effort – but it's worth it.

During the research phase, businesses should look for a provider with a standards-based environment and a high-level security program that meets its exact needs. This means you need to look at the contract and Service Level Agreement. Look for a provider that is transparent and willing to answer any questions you have. They should be able to validate that they meet certain compliance requirements with proof, and should be able to tell you exactly where your data will be located. Many regulations require proof that your data is located in the United States, so it's important to verify this fact with a provider.

You also need to look at access controls, because many regulations require you to prove how much access each user has, and how that access is maintained. A provider should have various levels of access controls in place and be able to describe the separation of duties between the different levels. This is another important factor in complying with many regulations.

Multi-tenancy is a security barrier for many organizations considering the cloud. Some organizations aren't even allowed to use this type of environment, due to the regulations they face. Those that can must have a provider prove its security measures that prevent one customer from accessing another customer's data. A provider should encrypt data in flight and at rest, and be able to share exactly how and when this encryption is applied.

A cloud provider really becomes an extension of a business' IT department. This makes it very important to complete thorough research before committing to a solution. Discover a cloud provider's security processes, incident response and disaster recovery procedures, issue escalation processes and more prior to committing. And once you've made the move, regularly check in on your compliance, as policies will continue to change over time. Maintain open communication with your provider, and include your IT team in the conversation. 91% said that their cloud providers were making it easier for them to meet government compliance requirements such as PCI, HIPAA, and SOX, so don't let compliance stop you from taking advantage of the cloud.

Key Considerations

Throughout the cloud planning process, organizations need to understand how the cloud will impact their IT environment, users, and overall business. Compliance won’t always be the sole barrier to deployment, so knowledge is key. Work closely with providers to receive compliance-ready cloud services, and keep security at the forefront of all discussions. As cloud computing continues to boom, there will only be more data and more targets, and next-generation security technology should continue to be implemented with all of this growth.

A cloud provider should be able to guide businesses through the planning and consideration process. You want more than a one-liner offering “compliant storage”. When looking for a reliable cloud provider, these are some key considerations:

- Recovery Assurance
- Automated Testing/Compliance Reports
- Current Compliance
- Digital Security (Encryption/Access Control)
- Regular Access Audits
- Verified Data Retention
- Secure Data Centers
- Service Level Agreements
- Segmentation Policies (For Multi-Tenant)

“91% said that their cloud providers were making it easier for them to meet government compliance requirements.”

RapidScale Data Centers and Security

In order to meet your security and compliance requirements in the cloud, you need to find a qualified provider. RapidScale delivers the highest quality protection for data and information. We have equipped ourselves with best-in-breed SAS70 Type II, SSAE 16-certified Tier 3 Class 1 data centers to hold your sensitive information for safe, encrypted storage.

Facilities Security

The fully redundant and geographically diverse data centers have the highest security parameters in place, and your information is secured behind multiple layers of both physical and network security. Only authorized data center personnel are granted access credentials to the facilities. No one else can enter the production area without prior clearance and an appropriate escort. Colo hybrid customers are only allowed with a RapidScale employee. Every data center employee undergoes multiple thorough background security checks before being hired. The facilities are fully redundant and feature multiple security measures including: key card protocols, biometric scanning systems including palm scanners, exterior security system, on-premises security guards, digital surveillance and recording, secured cages, around-the-clock interior, exterior surveillance monitor access and even bullet-proof glass.

Infrastructure and Storage

Our enterprise-grade infrastructure includes Cisco routers and firewalls with encryption-256k. We use NetApp encryption so all data is encrypted in flight and at rest. All SANs have self-encrypting drives (SEDs).

Environmental Controls

Every data center's HVAC (Heating Ventilation Air Conditioning) system is N+1 redundant. This ensures that a duplicate system immediately comes online should there be an HVAC system failure. Every 90 seconds, all the air in our data centers is circulated and filtered to remove dust and contaminants. Our advanced fire suppression systems are designed to stop fires from spreading in the unlikely event should one occur.

"94% of businesses reported they saw an improvement in security after switching to the cloud."

Additional

We give administrators access to remotely wipe any device that is lost or stolen and implement full credential-limited access to all data in the cloud. The virtual environment will log off within a set amount of time of inactivity, and in the event of device loss, users won't lose their critical data. It remains stored in the cloud where it's safe and accessible from a replacement device, as if nothing ever happened.

About RapidScale

RapidScale, a managed cloud services provider, delivers world-class, secure, and reliable cloud computing solutions to companies of all sizes across the globe. Its state-of-the-art managed CloudDesktop platform and market-leading cloud solutions are the reasons why RapidScale is the provider of choice for leading MSOs, VARs, MSPs, Carriers and Master Agents throughout the United States. RapidScale is not only delivering a service but also innovating advanced solutions and applications for the cloud computing space. RapidScale's innovative solutions include CloudServer, CloudDesktop, CloudOffice, CloudMail, CloudRecovery, CloudApps, and more.

For More Information Contact Us Today

Sales: (866) 371-1355
Support: (866) 686-0328
www.rapidscale.net