ONGOING OPERATIONS

# *Managing Security, Disaster Recovery & Compliance in the Cloud* Official White Paper

## Overview

Is my data safe? That's the number one question we field from prospective customers. It's on every customer's mind and if it isn't, it probably should be. Our customers facing compliance requirements (whether it be NCUA, SEC, FDIC, PCI, Sarbanes-Oxley, or HIPPA) take it one step further. They have to prove their data is safe and have processes in place to ensure it. Although some view it with suspicion, Cloud computing actually makes that job a little easier. A good Cloud provider will keep your data safe and they'll help you satisfy your auditors at the same time. It's all about the details, the benefits of the data center, having confidence in your provider's abilities, mitigating your risk, and obtaining a measurable bit of proof to make everyone sleep a little better at night.

## Physical Security, Environmental Controls, and Network Security

There are a few major components of security in Information Technology, physical security, environmental controls and network security. Each is important and each illustrates some of the real benefits of security in the cloud. Physical security is the easiest to communicate and the one that most people can understand and relate to. Most businesses have a need for physical security. They lock their doors, often have alarm systems, and sometimes surveillance cameras protecting their most valuable assets. Rarely however, do they consider their servers to be their most valuable assets. It's an oversight for sure, most businesses in an information economy store their most valuable assets on their computers but for some reason they don't protect them accordingly.

How many businesses have their servers in a location accessible to all staff and probably the evening janitorial crew? How many servers are located in glorified broom closets with the door left open to keep the room from overheating? How many are stuffed under someone's desk or in the break room? Maybe they are in a locked room, but who has the key? Do they even need a key? Can they just pop a few ceiling tiles and access the room through the drop ceiling? Your auditors have seen all of these conditions. In many industries these conditions are not the exception, they are the norm.

## Benefits of a Data Center

Physical security in the world of Cloud computing centers on the data center. Reputable Cloud providers run their services from professionally designed and managed data centers. It's really the only way to provide reliable computing 24/7, 365 days a year or as the IT industry describes it, with 99.9% or 99.99% uptime. Data centers are measured by how well they provide power, bandwidth, cooling and security. In fact, the industry has adopted a standard to classify the type of data center, Tier 1 through 4, based on how well prepared they are to provide these services. For more information, go to http://uptimeinstitute.org.

Higher tier data centers will deploy physical security measures such as two factor authentication, biometric scanners, video surveillance, and in some cases onsite security personnel, even armed guards. If a data center is shared by multiple customers they will typically segment the facility further to ensure that only authorized personnel have access to the specific areas where their systems are located. Equipment will be locked in cabinets and cages and those locks will be controlled by the customer. In short, there are multiple layers of physical security protecting customer data.

This type of physical security as well as some of the environmental protection (power and cooling redundancy) is something a customer could easily evaluate. And access controls should be documented. A reputable Cloud provider will maintain a list of who has access to the data center. That list should be kept up to date and it’s a list an auditor would love to look at now and then. You should also be able to request an escorted tour of our data center so you or your auditor can see for yourselves. If a cloud provider isn’t willing to do this, it might just be logistically difficult, or it might be a red flag.

### Environmental Controls

Another aspect of security that many customers overlook is environmental controls. Keeping data safe also means preventing it from being damaged or lost. Environmental controls such as reliable power and ample cooling are an important aspect of data protection. This is another benefit of a good data center. High quality power includes redundant power feeds with redundant UPS’s and often separate backup generators. Cooling is handled in a similar way. Each zone will have two separate coolers, each capable of cooling the area at peak loads. These characteristics help keep computer and network equipment happy and performing at optimum levels. That helps prevent failures and extend equipment life. That’s good for the customer and their data. And it’s worth noting, these types of environmental controls are entirely unaffordable for small and mid-market businesses. They simply can’t justify the millions of dollars in expense it takes to build out an environment like this, let alone manage it.

### Evaluating Network Security

Network security is bit more difficult to communicate. But the concept is a simple one. In our opinion, if a customer’s office network is connected to the outside world via an Internet connection, they share most of the same risks as a cloud provider. It’s that simple. So if the customer is better at network security than the cloud provider, then the customer should keep their data onsite. Odds are, however, they’re not. Most small and mid-market businesses don’t have network security professionals on staff. If they do, the cloud provider can engage them in a discussion of how security is provided and hopefully satisfy their concerns. If they don’t have a security expert on staff, there is an element of trust required. But you need not rely on trust alone.

Paradoxically, the more a cloud provider discloses about their internal security, the less secure they may be. There are some ways of gaining assurance that a cloud provider is managing the customer’s data properly. With an executed non-disclosure agreement, most cloud providers should be willing to provide details about how they secure their infrastructure. Another more objective source is an SSAE 16 report (SSAE 16 is the new audit standard that replaced SAS 70 in June of 2011). An SSAE 16 audit is similar to a financial audit in that it involves a third party auditor reviewing the internal processes and procedures of a firm and rendering an opinion. In the case of a SSAE 16 the report is on the controls of a service organization. In other words, is the service provider doing what they say they are doing? Cloud providers undergo these annual audits voluntarily. The result is an opinion rendered by a neutral third party that a customer and their auditors can review and evaluate without having to take the cloud provider's word alone as gospel.

Another document your auditor will appreciate is the results from a "pentest". Penetration tests evaluate computer and network security by simulating a malicious attack. The test searches for potential vulnerabilities that could result from incomplete or incorrect system configuration, hardware or software flaws, or operational weaknesses. The test results are like a network security "report card" that helps a cloud provider measure their own security controls and helps a customer to validate them.

A Cloud provider may provide the results of penetration tests for their entire environment. But because Cloud is typically a shared service, you may want to get a bit more specific. A better tool would be a pentest that was customized to focus just on the services you were interested in (i.e. your servers and your data). This test would be much more relevant and would be more informative to your auditor as well.

Ideally customers would be able to initiate a pentest on their own, at any time, and without the consent of the cloud provider. This offers a few advantages. It puts the customer in control of validating their environment. You or your auditors would be able to test at any time incorporating this into your own security protocols. It motivates the Cloud provider to maintain constant vigilance. And it benefits them by adding their customers to the ranks of their security team. The more people testing the environment, the more likely issues will be identified and resolved.

### Disaster Recovery

Among the benefits of Cloud computing is the ability to augment your production computing environment with disaster recovery capabilities at significantly lower costs than doing it on your own. But let's back up a bit. People tend to jump to the topic of Information Technology too quickly when discussing Disaster Recovery. Disaster Recovery really begins with some critical questions about your business such as: What type the most likely disasters you need to prepare for? What data and applications are critical to running your business? Who needs access to these applications and data? How quickly do you need to be back in operation? And how much data can be lost without serious consequences to the business?

These questions may be a part of a formal Business Impact Analysis. A BIA is a well defined process designed to prioritize business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result if your organization was to experience a business disruption. The results of a BIA are likely to increase demands of your Information Technology. When they do, the Cloud provides you with some options.

### The Risks in Geography

One of the fundamental tenets of Disaster Recovery is to put your eggs into a few different baskets. If you do business in a location that is susceptible to natural disasters (e.g. earthquakes, tornadoes, hurricanes) it is prudent to keep your data, or a copy of your data, in a location that is not likely to be affected by the same event. Cloud based backup is one way to address this requirement as it can place a copy of your data at a distant offsite location. Replication services provide additional protection by replicating your data and applications in near real-time to an appliance at your location and then, optionally, to a Cloud based data center as well. This protects you from minor problems such as a server failure as well as major events that disable your entire infrastructure.

The key metrics of Disaster Recovery are the time it takes to resume operations (the recovery time objective) and how much data you can tolerate losing in the process (the recovery point objective). For many businesses, restoring to last nights backup is the best case scenario, provided last nights backup ran properly. However, if your production computing environment is in the Cloud, your Disaster Recovery options are likely to improve, because to some degree, Disaster Recovery is inherent in the Cloud delivery model.

As we outlined in our discussion of the Data Center, many fault tolerance and redundancy features are designed into those facilities. Some Cloud providers will replicate their environments in different data centers in different parts of the country. In doing so, they protect themselves and their customers from events that may effect an entire data center or region of the country. If they don't do it by default, they may offer it to customers for an additional fee that is often far less than what it would cost to replicate your production environment on your own. This option could enable you to reduce your recovery time and recovery point objectives significantly.

**Business Risk Mitigation**
Another interesting option that some Cloud providers are offering is the ability to replicate the data you store in the Cloud back to your office location, in effect reversing the Cloud backup model. A perceived loss of control is one of the most common reasons decision makers cite as to why they are resistant to the Cloud. Some believe that even if their data is stored in a glorified broom closet down the hall, at least it is THEIR closet. If this sounds familiar, the ability to obtain all the benefits of the Cloud and to be able to replicate a copy of your data back to your beloved broom closet may provide you with the extra insurance you're looking for.

**Proving the safety of the Cloud**
Yes, the cloud is safe. That may seem like a bold statement especially when you consider that the cloud is not one thing. The Cloud is made up of hundreds of providers and not all of them are safeguarding your data equally. But we stand by that statement because in general, the characteristics of Cloud computing, such as top tier data centers, strong physical security, environmental controls, network security, and disaster recovery benefits are a big improvement over what most businesses typically provide on their own. **The key question about Cloud security is not whether it eliminates all risk, but whether the Cloud provider helps you manage risks better than what you are doing on your own.** Your auditor doesn't expect you to eliminate all risk, they expect you to identify and mitigate your risks. Cloud computing provides you with the tools to do. So when you evaluate a Cloud provider, think like an auditor and ask about:

- ✓ The data center
- ✓ Physical security
- ✓ Environmental controls
- ✓ Network security
- ✓ SSAE 16 report
- ✓ Penetration tests
- ✓ Disaster recovery

With the information obtained by asking some targeted questions and verified through a few reports, the job of compliance gets a whole lot easier. Not only for you, but for your auditor as well.