Just Because You Outsourced Your IT to the Cloud, Doesn’t Mean You Can Sidestep Your Risk Management Obligations

So how can you know if your Cloud Service Provider (CSP) has your best risk management interests in mind?

In a recent survey of 125 alternative asset management firms, nearly 80% are currently using cloud services from complete IT outsourcing to specific business functions or application hosting. Whether as a strategy to reduce costs, simplify management or improve time to market, cloud computing is here to stay. But as the cost of cloud services goes down, your risk profile goes up. Outsourcing IT services does not equate to off-loading or sidestepping your fiduciary responsibilities to your partners, investors, or other stakeholders. You are still required to provide financial governance, risk management and regulatory compliance. As a leading security service provider to alternative asset management firms, eSentire is securing hundreds of networks for hundreds of different customers in financial services whose aggregate AuM is greater than $750B.

The following document is for use by Hedge Funds and other financial institutions exploring the use of cloud-based services. This document is based upon the risk assessment standards and guidelines as outlined by the European Network and Information Security Agency (source: Cloud computing: Benefits, risks and recommendations for information security, 2009).

To learn if your Cloud Service Provider (CSP) is the weakest link in your risk management chain? Complete our CSP checklist and find out!

Contents
Physical Security................................. 4
Background Checks .............................. 5
Access and Change Control Audit........... 6
Vulnerability Assessment ...................... 7
Data Residence................................. 8
Business Continuity ............................ 9
Network Traffic and Access Logging ...... 10
Connections and Authentication .......... 11
Infrastructure................................. 12
Failover Site.................................. 13
1.0 Physical Security

**Does the cloud provider have a rigorous physical access protocol?**

- [ ] All secure areas are protected by demising walls
- [ ] All secure areas use card swipe technology to control access
- [ ] Sign in procedure for all third-party individuals (visitors, service providers, couriers, etc.)
- [ ] All visitors to secure areas (such as the COLO) must be escorted by authorized personnel at all times
- [ ] All employees, contractors, etc. must display security ID badges at all times
- [ ] All secure areas use card swipe technology to control access
- [ ] All secure areas use biometric scanners or other technology to control access
- [ ] All secure areas and perimeter areas are monitored 24x7x365 by CCTV

2.0 Employee and Contractor Background Checks

**Does the cloud provider have a rigorous physical access protocol?**

- [ ] Cloud provider performs criminal background check
- [ ] Cloud provider performs credit background check
- [ ] Cloud provider performs a confirmation of employment
- [ ] Cloud provider performs a confirmation of education and technical/industry credentials
3.0 Access and Change Control Audit (SSAE 16 SOC2 Type 2)

Does the cloud provider meet current SSAE 16 SOC2 Type 2 certification?

☐ The cloud provider is SSAE 16 SOC2 Type 2 compliant

☐ State the name of the CPA audit firm

☐ State the date of the most recent CPA audit

4.0 Vulnerability Assessment

Does the cloud provider perform regular vulnerability assessments to determine security gaps? This section also applies to any sub-contractors the cloud-provider uses as part of their service.

☐ State the date of the most recent Vulnerability Assessment

☐ Provide a comprehensive list of all security risks/gaps identified

☐ Have the security risks/gaps identified in the most recent VA been mitigated?
5.0 Data Residence, Persistence, Back-ups and Replication

Does the cloud provider have the proper processes, systems and services in place to ensure data integrity and persistence?

☐ Where is the data resident? Please list locations, state or country

☐ Are there any privacy or other legislation restricting the transmission and storage of data? Please describe.

☐ Are data back-ups stored on-site or off-site?

☐ If the data is stored off-site, does a sub-contractor store it? If so, please list all relevant contractors

☐ Is the data and storage media encrypted? Please describe.

☐ Is there controlled access to the data and storage media? Please describe.

6.0 Business Continuity

Does the cloud provider have a Business Continuity Plan in place?

☐ Describe the plan for power or critical service failure.

☐ Describe the plan for physical disasters such as fire, water damage or flooding as the result of a man-made or natural disaster.

☐ Describe the plan for civil disobedience encumbering operations, or government instability.

☐ Describe the plan for security breaches resulting in the failure of core systems, such as a Distributed Denial-of-Service (DDOS) attack.
7.0 Network Traffic and Access Logging

Does the cloud provider log network traffic, file and server access? All files should be made available to customers upon demand. Logs should record who accessed the system, by what route, what if any data was accessed or changed. Security event logs should be captured for the following items.

- Security systems (AV, UTM, ID/IPS)
- Network switches, routers, taps, etc.
- Databases and servers
- Active directory
- Web and mail servers
- VPN systems
- VM systems

8.0 Connections and Authentication

Does the cloud provider provide adequate security for network access and authentication?

- How are connections encrypted? (SSL, SSH, etc.)
- Are strong passwords required? If so, describe minimum requirements, expiration periods, etc.
- Is double-factor authentication used? If so, please describe.
9.0 Infrastructure

Does the cloud provider provide security measures for infrastructure, including sub-contractors?

☐ Is the service multi-tenant? Please describe.

☐ Is the service a dedicated colocation? Please describe.

☐ Is the service on segmented virtual machines? Please describe.

10.0 Failover Site

Does the cloud provider provide security measures for infrastructure, including sub-contractors?

☐ Is the failover site certified to the same standards as the primary facility? Please describe.

☐ Are the same security controls implemented at the failover site to the same standard as the primary site?

☐ Does the cloud provider employ an active-active configuration between the primary and failover site?
11.0 Customer Policy Enforcement

Does the cloud provider enforce policies required by their customer hedge fund?

☑ Can the cloud provider enforce your policies? Please describe.

☐ Are there any customer policies that cannot be enforced by the cloud provider (causing an audit exception)? If so, please describe.

12.0 SLA standards

Does the cloud provider have an active SLA in place that identifies minimum performance (such as up time) and any associated penalties for SLA breach?

☐ Describe the SLA.

☐ Describe penalties associated with SLA breach.
eSentire has reinvented enterprise network security by focusing on protecting your core assets inside the network through our human driven, behavior-based solution. We turn the traditional layered security approach on its ear as we assume your network is already compromised and focus from the inside out by detecting behaviors indicative of advanced threats from criminals, nation states or hactivists and even your own staff whether malicious or borne of ignorance. No matter where you are we have your back 24x7x365.