



Introduction to Cloud Services

(CS2)

KAPLAN



Course Audience

This course is designed for any professional with the desire to understand the basics of Cloud services and their use, impact and risk to an organization.



Program Topics

This program will cover:

- Cloud Services Basics
- Cloud Responsibility
- Cloud Risk and Security
- Privacy in the Cloud
- AICPA Ethics/Confidentiality to Consider with Cloud Services

3

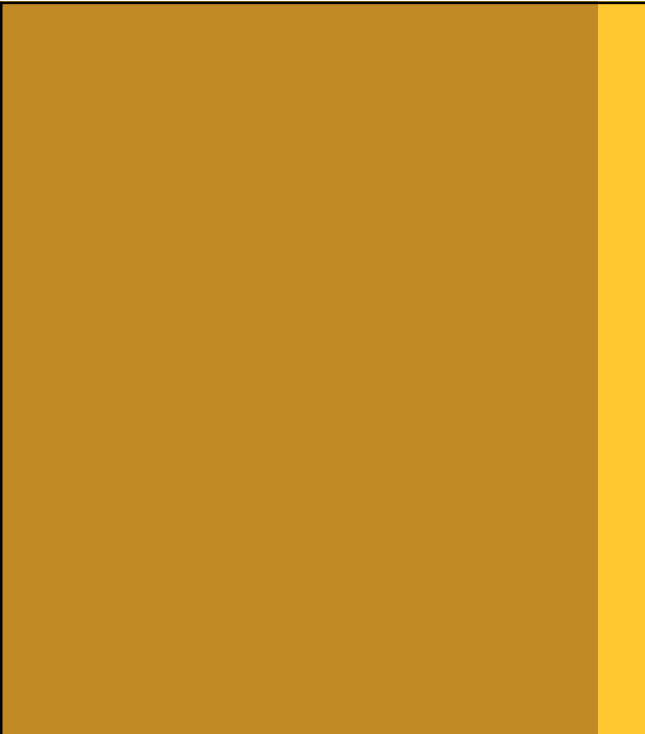


Learning Objectives

Upon course completion, participants will be able to:

- List the pros and cons of migrating to the Cloud;
- Define public, private, and hybrid Cloud types;
- Differentiate Cloud service models: IaaS, PaaS, SaaS;
- Recognize key risks involved with Cloud computing;
- Discuss how major privacy laws apply to the Cloud

4



Section 1 - Introduction: The Cloud - Where We Are Right Now

5



Course Overview

- With innovations in technology, the need for convenience and improving productivity, companies are increasingly outsourcing accounting and IT functions.
- Cloud computing has increasingly become a solution for organizations.
- Cloud computing removes the need for in-house IT infrastructure, provides faster implementation and instant access.
- This course provides CPAs an overview and background on cloud services, risks and compliance.

6



Key Terms

- **Cloud**
 - A third party's servers, network, data storage, infrastructure, software and virtual services provided to customers.
- **Service (Cloud) provider (also known as "CSP")**
 - The firm which provides Cloud services.
- **Tenant**
 - The customer that receives Cloud services. For purposes of this course, assume that the tenant is a business organization.

7



Introduction: The Cloud - Where we are Right Now

Today, clients and practitioners are flocking to put their sensitive data in the cloud. While using cloud services may be seen as a huge cost savings (no more on premises servers to maintain and defend, less overall resources required for IT, etc.), many IT experts will warn those who will listen that the cloud is really nothing more than putting all of your sensitive data on someone else's computer with all the possible negative consequences that can be imagined from that action, including possible loss or theft of that sensitive data.

8

Introduction: The Cloud - Where we are Right Now



Image Credit: <https://msdnshared.blob.core.windows.net/media/2017/06/image271.png>

9

Cloud Service, Deployment, and Responsibility Models

- Cloud Service Models – refers to the types of services provided
- Cloud Deployment Models – refers to how the cloud and services are provided
- Cloud Responsibility Models – refers to who owns responsibility for the various services provided

10



Three Cloud Service Models

- There are three **Cloud Service Models**, which refer to the level of services provided by a CSP (Cloud Services Provider) to a Tenant (Cloud Customer). (also, when more Cloud services are provided by the CSP, less on-premises services need to be maintained by the tenant.
 - **IaaS**: Infrastructure as a Service: The least amount of services that are provided by the CSP.
 - **PaaS**: Platform as a Service: More services are provided by the CSP.
 - **SaaS**: Software as a Service: Most services are provided by the CSP

11



Four Cloud Deployment Models

There are four major **Cloud Deployment Models**, which refer to the level of services provided by a CSP (Cloud Services Provider) to a Tenant (Cloud Customer). Also, when more Cloud services are provided by the CSP, less on-premises services need to be maintained by the tenant.

1. Public
2. Private
3. Hybrid
4. Multicloud

12



Four Cloud Deployment Models

1. **Public:** Look at this deployment as cloud storage shared with other tenants ("Multi-tenant". The shared Responsibility Model described below will usually apply for Cloud security matters. Inexpensive to set up, with very reasonable fractional pricing. Amazon Web Services ("AWS"), Microsoft Azure, and Google Cloud Services are notable Cloud Service Providers of Public Cloud solutions.
2. **Private:** In a nutshell, this is "your cloud", run on your servers which are generally located on the tenant's premises ("on-prem"). Your data is not stored in an environment with other tenants' data. Third party solution providers (such as Veeam) will assist tenants with managing Private Cloud solutions. This deployment is more expensive than Public above, and the tenant is responsible for Cloud security.

13



Four Cloud Deployment Models

3. **Hybrid:** Combination of Public/Private Cloud deployments, with some services remaining "on-prem" and other items stored on a public cloud. Financial institutions use a Hybrid cloud deployment strategy with the most client data stored on-prem and less confidential stored on a public cloud.
4. **Multicloud:** While technically not a Cloud Deployment Model, a Multicloud strategy will use two or more Public Clouds and/or two or more Public Clouds with a Private Cloud (a Hybrid Multicloud solution). The strategy behind a Multicloud solution is using the best individual service from a particular CSP; for example, using AWS for client interface tasks and Azure for virtual machines and Power BI.

14

Introduction: The Cloud - Where We are Right Now

Cisco says by 2021, 94 percent of all workloads will run in some form of cloud environment.

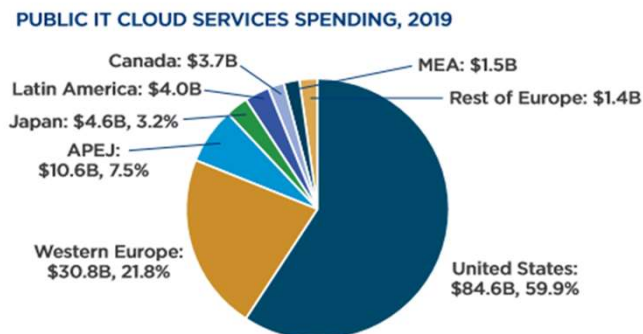
- COVID-19-related remote working accelerated this trend exponentially in 2020.
- In person office work will not return to pre-COVID levels, so a permanent level of remote work (whether it is 100% remote or a combination of remote/in office) will stoke exponential demand for Cloud services and related solutions for security, configuration, and collaboration.
- Continued demand after COVID: many remote workers will leave their current position if their remote work status changes back to in-person, and this group will even take a pay cut if given a choice to maintain their remote status versus going back to the office.

[Cisco says almost all workloads will be cloud based within 3 years | Network World](#)

15

The Cloud - Where We are Right Now

Spending for cloud services is increasing everywhere in the world:



#US40709515 - Worldwide and Regional Public IT Cloud Services Forecast, 2015-2019

16



Cloud Computing Trends Among CPA Firms

- 56 percent of CPA firms indicated they use cloud-based software.
- Cloud computing allows CPA to avoid traditional up-front infrastructure costs.
- Companies can use innovative technologies to improve workflows.

<https://www.aicpa.org/content/dam/aicpa/advocacy/state/downloadabledocuments/cloud-computing-one-pager.pdf>

17



Major Cloud Service Providers (CSPs)

- **As defined earlier, Cloud Services Providers (“CSPs”) are firms which offer a menu of cloud services (data storage, virtual services, etc.) There are three major players (by current market share) globally that provide cloud services:**
 - AWS (Amazon)
 - Azure (Microsoft Cloud)
 - Google Cloud Platform
- Other notable cloud providers include IBM Cloud, Hewlett Packard Cloud Services (HPE), Rackspace, Salesforce, SAP, VMware, Oracle Cloud, Box, Dropbox, and Egnyte, and Alibaba Cloud (China).
- Many smaller national or regional cloud providers throughout the world with a fraction of the revenues and client/ cloud user totals of those listed above.

18

Section 2 - Shared Responsibility Model And Vendor Lock-in

19

Shared Responsibility Model

Tenants **must** be familiar with two Cloud concepts: The Shared Responsibility Model and Vendor Lock-in, both described in detail in this section.

What is the Shared Responsibility Model ("SRM")?

- Arrangement that details which security obligations are those of the provider and which are owned by the tenants.
- Cloud services agreements use the SRM to allocate responsibilities between the CSP and the tenant.
- This document is a contract between a tenant and its CSP, and has characteristics of a user agreement, a terms and conditions clause, and a vendor contract or SLA (Service Level Agreement).

20

AT&T Definition of the Shared Responsibility Model

AT&T's AlienVault (now known as AT&T Cybersecurity) defines the Shared Responsibility Model on its website:

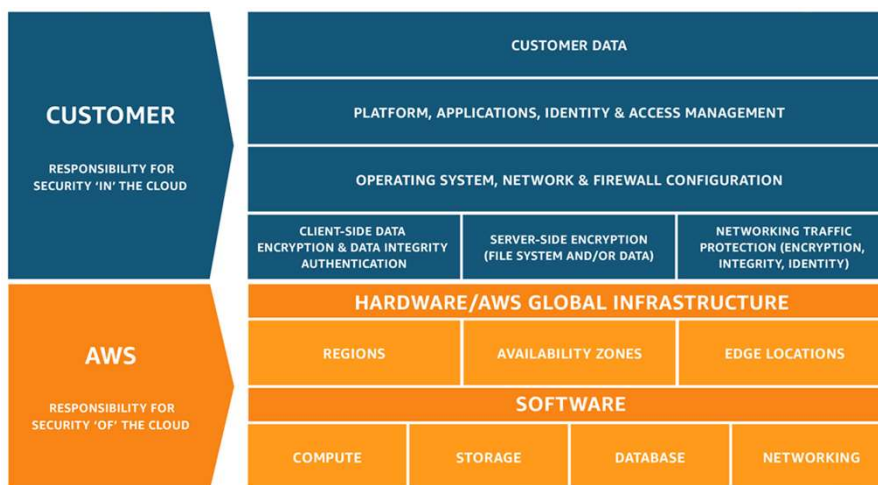
"As more companies move critical business applications to the cloud, security of those applications and data remains paramount. **But many companies are not aware of their responsibility for security in cloud environments such as AWS.** AWS operates on a shared responsibility model for security. This means that while Amazon secures its infrastructure, **the customer is responsible for the security of their applications, content, and systems.**"

- While most of the material here is from Amazon, all cloud providers generally use the AWS Shared Responsibility Model's requirements.

21

<https://cybersecurity.att.com/solutions/aws-shared-responsibility-model>

Shared Responsibility Model



22

Image credit: <https://aws.amazon.com/compliance/shared-responsibility-model/>



Customer (Tenant) Responsibility

- The Shared Responsibility Model is comprised of two major parts: the Tenant's security responsibilities and CSPs the security responsibilities.
- Tenant's (Customer) responsibilities – **"security in the cloud"**:
- ****Customer Data:** The **tenant** is responsible for all of its data uploaded to the cloud, including its confidential data (taxpayer/healthcare/employee/ personally identifiable information, etc.).
 - Treat the security of the data uploaded to the cloud just as you would if the data was on-prem (hopefully not on a local workstation).
 - Review with counsel all applicable laws and regulations relating to data breach/data privacy for your data and use appropriate security measures.

23



Customer (tenant) Responsibility

- The customer's (tenant's) responsibility is determined by the services the customer uses and **must be configured by the customer** to ensure security of the system.
- These services include customer data, OS (Operating system), network, firewall configuration, client-side data, encryption and data integrity, and server-side encryption. Identity Access Management (IAM) is an important part as well.
- **Service & Communications Protection/Zone Security:** Customer routes or zones data within specific security environments

<https://awsnewbies.com/shared-responsibility-model/>

24



Customer (Tenant) Responsibility

- The tenant should **at a minimum** perform the following security measures:
 - Install end point security
 - Encrypt all confidential data
 - Monitor its data flows
- A third-party vendor may be the best entity to provide these security services.
- The tenant is also responsible for several configurations.
- The concept of the shared responsibility model is explored in more detail in the definitions section but ensure that you have read and that you understand your responsibilities under the model.
- Consult with counsel as well.

25



Cloud Provider's (CSP's) Responsibility

CSP is responsible for the hardware, software, networking and facilities that are involved in running the Cloud.

The cloud provider is **not** responsible for any point in the process outside of the cloud location/s itself.

According to Amazon:

- **AWS is responsible for security OF the cloud.**
- **The customer is responsible for security IN the cloud.**

<https://awsnewbies.com/shared-responsibility-model/>

26



Shared Responsibility Model: Lock Your Door!

Amazon further explains the model on its website:

- A good question to ask is: “Can I log in and adjust the security settings?” If **yes**, then it’s **your** responsibility. If not, then it’s AWS’s responsibility.

Fully Controlled by AWS

- Physical and Environmental Controls

Shared Controls

- AWS provides requirements for infrastructure and customer provides its own control implementation.

<https://awsnewbies.com/shared-responsibility-model/>

27



Vendor Lock-in

What is the Vendor lock-in (“VLI”) concept?

VLI occurs when a CSP creates circumstances which make it very difficult and expensive to switch from it to another CSP. While VLI can theoretically apply to any vendor, an organization can be severely affected by a CSP VLI situation.

28



Vendor Lock-in

Why is VLI so painful?

- Tenants move large databases to the cloud for security, business continuity, and remote access (especially over the past year). Tenants get accustomed to the CSP and its procedures, and the resulting relationship is one of dependency. The longer the relationship has been established, the greater the degree of dependency.
- Migrating a database or similar formatted data to the cloud from an on-prem traditional data center is costly in terms of expenses and IT resources. To move this data a second time to a new CSP with differing configuration requirements, different software, and separate formatting standards can be as expensive and complex as the original migration. A second round of training for tenant employees will likely be required.

29



Vendor Lock-in

Indicators of a Bad CSP

- The CSP's service quality is decreasing (unanswered emails, unanswered or delayed help desk responses, etc.) and the tenant
- The tenant has different needs since first contracting with the CSP, but the CSP will not change its practices in response (i.e., the CSP's pricing is higher than other CSPs and it will not budge in this area after several increases, or its technology is outdated compared to its competitors).

30



Vendor Lock-in: How To Avoid VLI

Cloudflare explains how to best avoid or minimize cloud vendor lock-in by taking the following steps:

- **Evaluate cloud services carefully:**

- Companies should thoroughly research a cloud vendor before they make a commitment, ideally with a proof of concept deployment to make sure that their level of service is sufficient. Note that there isn't much choice for public clouds as three major players make up over 80% of the market.

- **Ensure data can be moved easily:**

- Tenants should make an effort to keep their data portable, or easy to move from one environment to another. They can partially do this by clearly defining their data models and keeping data in formats that are usable across a variety of platforms, rather than formats that are specific to a given vendor.

31 <https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/>



Vendor Lock-in: How To Avoid VLI

- **Backups:** Keeping internal backups of all data helps a business stay ready to host the data elsewhere if it is too difficult or time consuming to extract it from cloud service (as well as providing some protection from ransomware).
- **Multicloud or hybrid cloud strategy:** A multicloud approach incorporates multiple cloud providers, reducing dependence on any single vendor. In a hybrid cloud, some data will remain within an organization's direct control, either in a private cloud or stored on-premises.

32



Discussion Question 1

Which of the following statements is true:

- a. The Cloud Customer is responsible in all instances for the security of its data in the cloud.
- b. The Cloud Provider is responsible in all instances for the security of the Cloud Customer's data in the cloud.
- c. Both the Cloud Customer and Cloud Provider assume responsibility respectively for the security of the Cloud Customer's data in the cloud, and these responsibilities are set out in a Shared Responsibility Model document.
- d. The Department of Homeland Services, through its Cybersecurity Division, is ultimately responsible for the security of data uploaded to any cloud.

33



Discussion Question 1 Answer

Which of the following statements is true:

- a. The Cloud Customer is responsible in all instances for the security of its data in the cloud.
- b. The Cloud Provider is responsible in all instances for the security of the Cloud Customer's data in the cloud.
- c. **Both the Cloud Customer and Cloud Provider assume responsibility respectively for the security of the Cloud Customer's data in the cloud, and these responsibilities are set out in a Shared Responsibility Model document.**
- d. The Department of Homeland Services, through its Cybersecurity Division, is ultimately responsible for the security of data uploaded to any cloud.

34



Section 3 – Cloud Risk And Security



Cloud Risk and Security

- With any technology there are risks. This is no different with Cloud technology. There are many risks which can be mitigated with the proper controls.
- As society continues to migrate to remote cloud-based workforces during our COVID era, we cannot let our collective guard down with cloud security.
- The Cloud security threat landscape is comprised of:
 - All threats around unauthorized access that would be found in an on-premises environment.
 - All cybersecurity threats (see separate section for cybersecurity risks).
 - Threats that are specific to the cloud (more so for public clouds, which are less secure).

Let's look at these threats and see how we can mitigate against them.

36



Cloud Security

- According to recent research, 1 in 4 users of public cloud services has experienced data theft by a malicious actor.
- An additional 1 in 5 has experienced an advanced attack against their public cloud infrastructure.
- In the same study, 83% of organizations indicated that they store sensitive information in the cloud.
- With 97% of organizations worldwide using cloud services today, it is essential that every one of them evaluates their cloud security and develops a strategy to protect their data

<https://www.mcafee.com/enterprise/en-us/security-awareness/cloud.html>

37



Cloud Security: Mitigation Against Threats

Common cloud-specific mitigation techniques include:

1. **Access:** know who has access to your cloud and APIs (APIs are the “windows” used to observe what is going on in your cloud)– check this list at least every six months and update for any personnel changes (separations/new hires/promotions). Which vendors have access? Access should be as limited as possible, and a reason should exist for the access. Ideally, a tool is monitoring access in real time and is generating alerts for unauthorized access and other anomalies.

38



Cloud Security: Mitigation against threats

Common cloud-specific mitigation techniques include:

2. **Monitoring and Cloud Usage Visibility:** designate a person to review logs which indicate who, when and where the cloud was accessed. Some providers have tools which monitors and generates alerts for access, among other items. (Example: AWS Cloudwatch)

39



Cloud Security: Mitigation against threats

Common cloud-specific mitigation techniques include:

3. **Configuration and Change Control: Ensure that default settings have been turned off/changed!** Use a cloud configuration management tool to monitor configuration and security settings in real time. Ensure that a human reviews configuration and change logs on a regular basis, and confirm that this person receives alerts for unauthorized changes.

40



Case examples of cloud-based data breaches

The following sub-section covers two major cloud-based data breaches with details on their origins.

41



Cloud Hopper



ations, from IBM to Hewlett Packard Enterprise to Fujitsu, were invaded by Chinese cyber spies, Reuters found. Illustration by Catherine Tai/REUTERS

Eight of the world's biggest technology service providers were hacked by Chinese cyber spies in an elaborate and years-long invasion, Reuters found. The invasion exploited weaknesses in those companies, their customers, and the Western system of technological defense.

By JACK STUBBS, JOSEPH MENN and CHRISTOPHER BING | Filed June 26, 2019, 6 a.m. GMT

<https://www.wsj.com/articles/ghosts-in-the-clouds-inside-chinas-major-corporate-hack-11577729061>
<https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/>

42



Cloud Hopper

How did these attacks take place? According to the DOJ indictment, the Chinese attackers targeted MSPs and used spearfishing and social engineering techniques to gain access:

- Members of the conspiracy sent customized emails to intended targets with attached documents and files that would surreptitiously install malware if opened.
- The emails purported to be sent from legitimate email addresses, when in fact the emails were sent by members of the conspiracy.
- The content of the email messages and the filenames of the attachments appeared to be legitimate and contain information of interest to the recipients.

43



Cloud Hopper

- For example, one spear phishing email, which was sent to employees of a victim company ("Victim-2") involved in helicopter manufacturing, had the subject line **"C17 Antenna problems,"** which was a malicious Microsoft Word attachment named "12-204 Side Load Testing.doc," and stated the following:

"Please see the attached the files."

- When the attachment named "12-204 Side Load Testing.doc" was opened, malware was installed on the computer of Victim-2.

<https://www.justice.gov/opa/press-release/file/1121706/download>

44

Cloud Hopper

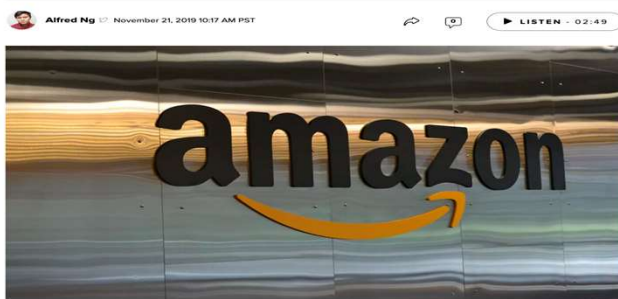
CPAs should absolutely question their Cloud Service Providers and, if applicable, their MSPs (Managed Service Providers) to check if they have been affected in any way by any of the Cloudhopper attacks.

45

Capital One / AWS Data Breach

Amazon tells senators it isn't to blame for Capital One breach

Sens. Elizabeth Warren and Ron Wyden have called for an investigation of Amazon, which hosted a cloud server used by the banking giant.



46

<https://www.cnet.com/news/amazon-tells-senators-it-isnt-to-blame-for-capital-one-breach/>



Capitol One/AWS Cloud Breach

Seattle-area woman Paige Thompson stands accused of leveraging a misconfigured web application firewall to access the finance company's files, hosted on Amazon Web Services (AWS) S3 servers (criminal complaint here: – adult language used in complaint):

<https://www.justice.gov/usao-wdwa/press-release/file/1188626/download>

47



Capitol One/AWS Cloud Breach

- The breached cloud storage buckets contained data that Americans and Canadians filled out on their credit card application forms, including names, addresses, zip/postal codes, phone numbers, email addresses, birth dates and self-reported income.
- Other compromised data included credit scores, credit limits, balances, payment histories, contact information, fragments of transaction data and, in a small subset of cases, Social Security numbers, linked bank account numbers and social insurance numbers

<https://www.scmagazine.com/home/security-news/capital-one-breach-exposes-not-just-data-but-dangers-of-cloud-misconfigurations/>

48



Capitol One/AWS Cloud Breach

- The breached cloud storage buckets contained data that Americans and Canadians filled out on their credit card application forms, including names, addresses, zip/postal codes, phone numbers, email addresses, birth dates and self-reported income.
- Other compromised data included credit scores, credit limits, balances, payment histories, contact information, fragments of transaction data and, in a small subset of cases, Social Security numbers, linked bank account numbers and social insurance numbers

<https://www.scmagazine.com/home/security-news/capital-one-breach-exposes-not-just-data-but-dangers-of-cloud-misconfigurations/>

49



Cloud Services Security in HR/Payroll

Scary Clouds: Payroll

NY Payroll Company Vanishes With \$35 Million

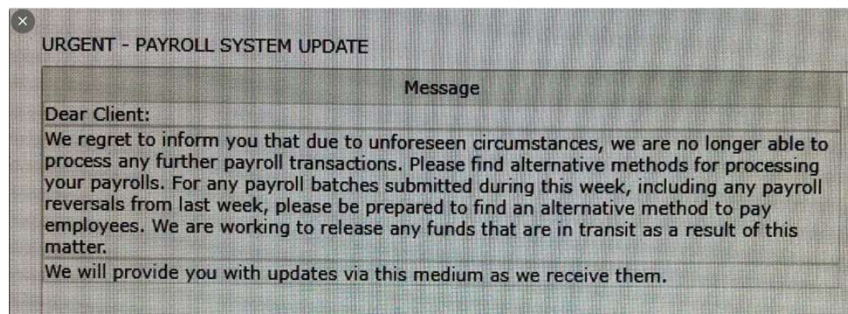
- Serves as a warning to other payroll providers about how quickly and massively things can go wrong when a **trusted cloud partner unexpectedly turns rogue.**

(this section taken from Krebs on Security, <https://krebsonsecurity.com/2019/09/ny-payroll-company-vanishes-with-35-million/>)

50

Cloud Services Security In HR/Payroll

This communique came after employees at companies that depend on MyPayrollHR to receive direct deposits of their bi-weekly payroll payments **discovered their bank accounts were instead debited for the amounts they would normally expect to accrue in a given pay period.**



51

<https://krebsonsecurity.com/2019/09/ny-payroll-company-vanishes-with-35-million/>

Cloud Services Security in HR/Payroll

- Access controls for HR/Payroll areas should be identical and should include:
 - Multi-factor authentication level;
 - Strict access controls with limited access to HR/Payroll data wherever it is located;
 - Periodic review of access control logs relating to systems/applications/networks/vendor portals;
 - Limited access permissions and rights to a few trusted employees;
 - Encryption of HR/Payroll data at rest and in transit
 - Review of vendor contracts within this area, with the requirement of a minimum level of security as well as a statement of compliance with any applicable state, federal, or other privacy/breach notification laws (NYDFS, HIPAA, GDPR, etc.);
 - Backup and retention policies over this confidential data should be in place with a rationale for implementation.
 - Always monitor your payroll account/s for abnormal activity, especially any abnormal withdrawals

52



Section 4 – Privacy in the Cloud

53



Privacy in the Cloud

- Data Privacy is an emerging area of law and technology
- Data Privacy and Data Breach Notification laws exist at the state and federal levels in the US, and at regional (GDPR), national and provincial (Germany and Canada) jurisdictions worldwide
- All tenants must follow these laws closely to comply with all applicable requirements or fines, penalties and reputation damage may result!

54



Privacy in the Cloud

- The most prominent US state privacy laws are:
- California Consumer Privacy Act (CCPA)
 - Many states updated their data privacy and breach notification laws to resemble CCPA
- New York state privacy laws, including:
 - NY SHIELD/privacy
 - NYDFS/state cybersecurity law for certain industries
 - New York State healthcare privacy law
 - NY state legislators have drafted a 4th major data privacy bill in 2021 based on the CCPA model which may pass in the next few months

55



Privacy in the Cloud

Geographic Compliance

- Most Public Cloud systems are international and this brings many benefits.
 - The data can be accessed worldwide with minimal latency,
 - There are remote backup copies of data which would be unaffected by natural disasters at a particular location
 - The CSP can keep prices low by using sites in countries with lower costs.
- There are risks which come with international storage and these should be assessed and, if possible, mitigated through SLAs (service level agreements) and contracts.

56

<https://social.technet.microsoft.com/wiki/contents/articles/3800.compliance-issues-in-the-cloud.aspx>



Privacy in the Cloud

Privacy compliance laws at the US Federal level, based on industry

- Graham Leach Bliley Act (GLBA): financial industry
- Payment Card Industry Data Security Standard (PCI-DSS): credit card standard
- Health Insurance Portability and Accountability Act (HIPAA): healthcare
- Family Educational Rights and Privacy Act (FERPA): students/educational institutions

57



Privacy in the Cloud

- In order to determine the relevant privacy laws which may apply to your cloud data, confirm with your CSP where your data is created, copied, stored, and transferred through, (region, country, state/province). A general term for all of these terms except create is “processed”.
- You must also know where the data subject resides (the data subject is the owner of the data – this data usually includes the data subject’s personal characteristics and his/her confidential unique identity data).
- Under the GDPR, “data processing” can be as minimal as briefly viewing the IP address of an identifiable GDPR-covered data owner on a terminal screen

58



Privacy in the Cloud

Incident Response Plan (IRP)

This is a set of instructions to assist staff in detecting, responding to and fixing network security incidents.

- Confirm with counsel as to which privacy laws apply to your company and Cloud arrangements.
- Include the relevant privacy laws within the IRP.
- Include breach notification requirements within the IRP.

59



Privacy in the Cloud

Compliance factors relating to the Cloud

- Generally, data privacy laws will include requirements which are derived from the following areas:
 - Cloud platform integrity and security – on the CSP side. How often is this tested?
 - Access to APIs, applications/any access to the cloud
 - Privileged user/Superuser access
 - Data storage locations – data at rest, in transit, in use – don't forget backups
 - Monitoring, reporting, and auditing tools (must be automated and real-time with alerts)
 - Data retention/backup policies of the CSP (especially at the end of the tenant-CSP contract).

60



Privacy in the Cloud

Compliance and Contracts

- Information Requests
 - How are information requests, including subpoenas, from legitimate authorities (e.g. government and police) to be handled? Step by step policies and procedures on both the tenant and CSP side are important for this critical area.
 - How much data and which data will be released for a particular request/subpoena? At a minimum, logging and monitoring data will be needed.
 - Retention periods are very important here as well.

61



Privacy in the Cloud

The CLOUD Act (Clarifying Lawful Overseas Use of Data (CLOUD) Act

- In 2018, Congress passed the CLOUD Act, which requests data held in the cloud for a particular tenant.
- The Cloud Act updates the legal framework for United States law enforcement requests for data stored on the servers of communication and CSPs, and allows for a limited mechanism for United States law enforcement to request data stored in the United States and overseas.

<https://aws.amazon.com/compliance/cloud-act/> <https://www.dailydot.com/debug/cloud-act-internet-rights/>

62



Privacy in the Cloud

The CLOUD Act (Clarifying Lawful Overseas Use of Data (CLOUD) Act

- Creates additional safeguards for cloud content, including under a new option for the United States to enter into executive agreements with other countries governing law enforcement requests.
- Apple, Facebook, Google, Microsoft, and Oath wrote in a letter in February that the CLOUD Act “provides a logical solution for governing cross-border access to data”.

<https://aws.amazon.com/compliance/cloud-act/> <https://www.dailydot.com/debug/cloud-act-internet-rights/>

63



Privacy in the Cloud

The CLOUD Act (Clarifying Lawful Overseas Use of Data (CLOUD) Act

- Before the law was passed, it was described by privacy advocates as essentially being a backdoor to access data without respecting privacy laws in various countries.
- The Electric Frontier Foundation (EFF) stated that the “...U.S. and foreign police will have new mechanisms to seize data across the globe...” “Because of this failure, your private emails, your online chats, your Facebook, Google, Flickr photos, your Snapchat videos, your private lives online, your moments shared digitally between only those you trust, will be open to foreign law enforcement **without a warrant** and with few restrictions on using and sharing your information. Because of this failure, U.S. laws will be bypassed on U.S. soil.”

<https://www.dailydot.com/debug/cloud-act-internet-rights/>

64



Cloud Security Alliance

CSA – Cloud Security Alliance

- Well-known non-profit entity whose primary purpose is to improve cloud security.
 - Offers several cloud security certifications and accreditations and also features several best practices publications as well as its own Security Trust Assurance and Risk (STAR) Program and Cloud Controls Matrix (CCM) frameworks.
- World's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.
- Harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products.
- CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

<https://cloudsecurityalliance.org/>

65



Privacy in the Cloud

Privacy Exercise

LionDive, Inc., a healthcare provider which processes patient data, is considering migrating to the cloud, and they would like some guidance on what they should do – What type of cloud deployment model should be used and why?

66



Privacy in the Cloud

Privacy Exercise Answer

Cloud type: To balance both cost savings and security for their confidential patient data, LionDive should consider a hybrid cloud solution. The public cloud deployment could be used for processing and storing all non-patient data at a significant cost savings over their current on-prem setup. A private cloud solution should satisfy regulatory requirements, including HIPAA relating to patient data security.

67

Section 5 - AICPA Ethics/ Confidentiality Rules

68



AICPA Confidentiality Rules

AICPA ETHICS: AICPA Code of Professional Conduct, Section 1.700.001– CPAs must consider these items with any security incident occurrences caused by unauthorized access or theft of client data located in the cloud or elsewhere. As always, confirm with competent counsel.

69



AICPA Ethics

Confidential Client Information Rule under Section 1.700.001

- **391/Interpretation 391-2, “Disclosure of Client Information to Third Parties”**
- **Regs. Secs. 301.7216-1 through 301.7216-3**
- 1.700.005, “Application of the Conceptual Framework for Members in Public Practice and Ethical Conflicts”;
- 1.700.010, “Client Competitors”;
- 1.700.020, “Disclosing Information From Previous Engagements”;
- 1.700.030, “Disclosing Information to Persons or Entities Associated With Clients”;

70

<https://www.journalofaccountancy.com/issues/2015/mar/aicpa-confidentiality-rule.html>



AICPA Ethics

Confidential Client Information Rule under Section 1.700.001

- 391/Interpretation 391-2, "Disclosure of Client Information to Third Parties"
- Regs. Secs. 301.7216-1 through 301.7216-3
- 1.700.040, "Disclosing Information to a Third-Party Service Provider"
 - .01 When a member uses a third-party service provider (**CSP/Cloud Services Provider**) to assist the member in providing professional services, threats to compliance with the "Confidential Client Information Rule" [1.700.001] may exist.

<https://www.journalofaccountancy.com/issues/2015/mar/aicpa-confidentiality-rule.html>

71



AICPA Ethics

Confidential Client Information Rule under Section 1.700.001

- 391/Interpretation 391-2, "Disclosure of Client Information to Third Parties"
- Regs. Secs. 301.7216-1 through 301.7216-3
- 1.700.040, "Disclosing Information to a Third-Party Service Provider"
 - .02 Clients may not expect the member to use a third-party service provider to assist the member in providing the professional services. **Therefore, before disclosing confidential client information to a third-party service provider, the member should do one of the following: Part 1 — Members in Public Practice 140**
 - a. Enter into a contractual agreement with the third-party service provider to maintain the confidentiality of the information and provide reasonable assurance that the third-party service provider has appropriate procedures in place to prevent the unauthorized release of confidential information to others.

<https://www.journalofaccountancy.com/issues/2015/mar/aicpa-confidentiality-rule.html>

72



AICPA Ethics

Confidential Client Information Rule under Section 1.700.001

- 391/Interpretation 391-2, "Disclosure of Client Information to Third Parties"
- Regs. Secs. 301.7216-1 through 301.7216-3
- 1.700.040, "Disclosing Information to a Third-Party Service Provider"
 - .02 Clients may not expect the member to use a third-party service provider to assist the member in providing the professional services. **Therefore, before disclosing confidential client information to a third-party service provider, the member should do one of the following: Part 1 — Members in Public Practice 140**
 - a. (continued) The nature and extent of procedures necessary to obtain reasonable assurance depends on the facts and circumstances, including the extent of publicly available information on the third-party service provider's controls and procedures to safeguard confidential client information.

<https://www.journalofaccountancy.com/issues/2015/mar/aicpa-confidentiality-rule.html>

73



AICPA Ethics

Confidential Client Information Rule under Section 1.700.001

- 391/Interpretation 391-2, "Disclosure of Client Information to Third Parties"
- Regs. Secs. 301.7216-1 through 301.7216-3
- 1.700.040, "Disclosing Information to a Third-Party Service Provider"
 - .02 Clients may not expect the member to use a third-party service provider to assist the member in providing the professional services. **Therefore, before disclosing confidential client information to a third-party service provider, the member should do one of the following: Part 1 — Members in Public Practice 140**
 - b. Obtain specific consent from the client before disclosing confidential client information to the third party service provider. **Confirm if the CSP has/ does not have access to your client data**

<https://www.journalofaccountancy.com/issues/2015/mar/aicpa-confidentiality-rule.html>

74



AICPA Code Of Professional Conduct, Section 1.700.001

Confidential Client Information Rule under Section 1.700.001

- 1.700.050, "Disclosing Client Information in Connection With a Review of the Member's Practice";
- 1.700.060, "Disclosure of Client Information to Third Parties";
- 1.700.070, "Disclosing Client Information During Litigation";
- 1.700.080, "Disclosing Client Information in Director Positions";
- 1.700.090, "Disclosing Client Names"; and
- 1.700.100, "Disclosing Confidential Client Information as a Result of a Subpoena or Summons."

75

Appendix A - Cloud Services Audit Exercise

76



Exercise: Cloud Services Audit

LionDive Enterprises, a major client, has engaged your firm to perform a readiness review to prepare for a future IT Audit that their largest client has requested. LionDive has gradually migrated some of their most critical data to AWS over the past three years and they have performed any internal or external testing on the migration.

77



Exercise: Cloud Services Audit

What subject areas should you be scoping into the readiness engagement? Consider data location, your firm's security, the SLA, applicable laws, and AWS services the client uses.

78



Exercise: Cloud Services Audit Answer

(This is a short summary of a cloud services audit)

Cloud Services & Scoping

Identify the **Cloud Services Provider (CSP)** and any additional cloud-related service vendors (v-CISO/MSSP).

- Obtain the **CSP agreement** and any additional vendor agreements/SLAs related to cloud privacy/security services.
- **Personnel** – Identify all employees, contractors and vendors related to cloud services received: CISO/IT, MSSP, Dedicated Cloud team, Legal, HR, Sales/Marketing, Internal Audit/IT Audit, Finance/Accounting, and DevOps team may need to be included.

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

79



Exercise: Cloud Services Audit Answer

Cloud Services & Scoping

- Review the **CSP service map and the internal inventory of cloud services** Ensure that **all services listed in the inventory are listed in the service map**.
 - A service map is a listing of cloud-based services (e.g., Virtual Machines) matched to a description and then to the actual CSP product name for that service (see next slide).

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

80

Example of a Service Map (Azure and AWS services comparison)

Service	Description	AWS	Azure
Virtual servers	Allows users to deploy, manage, and maintain OS and server software; instance types provide configurations of CPU/RAM.	Elastic Compute Cloud (EC2) VMs	Virtual Machines
	Offers a lightweight, simplified product offering users can choose from when building out a virtual machine.	Amazon Lightsail	Virtual Machine Images
Container management	Supports Docker containers and allows users to run applications on managed instance clusters.	EC2 Container Service (ECS)	Container Service
	Allows customers to store Docker formatted images. Used to create all types of container deployments on Azure.	EC2 Container Registry	Container Registry
Microservice-based applications	Orchestrates and manages the execution, lifetime, and resilience of complex, interrelated code components that can be either stateless or stateful.		Service Fabric
Backend process logic	Integrates systems and runs backend processes in response to events or schedules without provisioning or managing servers.	Lambda	Functions
			Event Grid

Image credit: <https://azurecomcdn.azureedge.net/mediahandler/acomblog/media/Default/blog/41be757c-31dd-49a5-a0aa-fec40f2a752a.png>

81

Example of an Inventory of Cloud Services document (Azure Resource Graph)



Image credit: [Quickstart: Your first portal query - Azure Resource Graph | Microsoft Docs](#)

82

Second Example of an Inventory of Cloud Services Query (Azure Resource Graph)

Show resources that contain storage

Instead of explicitly defining the type to match, this example query will find any Azure resource that `contains` the word `storage`.



Image Credit: [Starter query samples - Azure Resource Graph | Microsoft Docs](#)

83

Exercise: Cloud Services Audit Answer

Governance

- Obtain the most recent third party attestation performed on the CSP and confirm that the attestation includes the services that LionDive uses (most likely a SOC 2). **Also obtain the most recent LionDive attestation report, and confirm that all cloud service controls have been included.**
- **Obtain the most recent risk assessment, and confirm that cloud services were included.**

Credit: [Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

84



Exercise: Cloud Services Audit Answer

Access Management

- Obtain a list of users with cloud access, validate their privileges are in line with their roles.
- Obtain the cloud password/certificate/tokens policies, validate through a sample of users that they are compliant (check if there is a way to continuously monitor this) or ideally, **federated** (similar to Single Sign On, which allows one user ID and password to be used across multiple systems) to existing systems.
- Validate that access to the cloud is approved by appropriate personnel.
- Verify that periodic review of cloud users is preformed accurately and completely; is access updated when employees move between roles or leave LionDive?

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

85



Exercise: Cloud Services Audit Answer

Data Security

- Understand what data the LionDive has in the cloud and where the data resides, and validate the methods used to protect the data at rest and in transit (also referred to as “data in-flight” or “in motion”).
- Inquiry: ask if LionDive has asked its CSP for evidence that LionDive’s data doesn’t go where it’s not supposed to. Is it part of the contractual obligation?
- Determine what is in scope regarding regions and legislation. What CSP regions/countries are being used? What regional/global legislation should be considered?

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

86



Exercise: Cloud Services Audit Answer

Data Security

- Review the procedure for conducting a specialized wipe prior to deleting the volume for compliance with established requirements (e.g., every state has its own data disposal statute). This is to ensure deletion of LionDive data.

Network

- Understand the CSP security requirements and what the CSP requires of each of its customers.

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

87



Exercise: Cloud Services Audit Answer

Network

- Understand the connectivity with the cloud and if that traffic is encrypted. What can connect? User devices? VPN? Direct network connections? Are the connections appropriate? Are their limiting security rules to scope connectivity down to the minimum required? Who has access to configure and change VPN settings?
- Verify that LionDive has a procedure for granting remote, Internet or VPN access to employees for CSP Console access **as well as remote access to networks and systems**. Obtain evidence demonstrating that there is **only one way to provision access and that it hasn't changed over time**.

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

88

Exercise: Cloud Services Audit Answer

User Device Management

- Inquiry: Has LionDive asked its CSP for evidence that LionDive's data doesn't go where it's not supposed to (are there virtual barriers to separate the tenant's data from other tenant's data – what about backup copies?) Is this part of the contractual obligation?
- Determine what's in scope regarding regions and legislation. What CSP regions/countries are being used? What regional/global legislation should be considered? Ensure that all countries are covered (all countries where the data is processed, stored, or transferred through).

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

89

Exercise: Cloud Services Audit Answer

User Device Management

- Review a copy of the mobile device management policy (MDM).
- Does the MDM allow for employees to use their own devices, (BYOD) *especially with our current COVID remote work situation*? If so:
 - What are the policies and requirements, especially with processing personal data? If personal devices are used for accessing email, is copying/pasting/downloading blocked?
 - Does LionDive have management profiles on user mobile devices?
 - How are user devices managed?
 - How are employees handling operating system updates (especially on BYOD devices)?

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

90



Exercise: Cloud Services Audit Answer

Configuration Management

- Validate that the operating systems and applications are designed, configured, patched and hardened in accordance with CSC policies, procedures, and standards. Confirm that all OS (Operating System) and application management practices can be common between on-premises and cloud systems and services.
- What changes are the responsibilities of LionDive versus the CSP? For example, LionDive may be responsible for change request, UAT (User Acceptance Testing), and change deployment whereas the CSP could be responsible for development and integration testing.
- For changes that LionDive is responsible for, are there sufficient change management controls in place to ensure that management expectations are met and risks are addressed (this should be addressed in the risk assessment)?

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

91



Exercise: Cloud Services Audit Answer

Vulnerability Management

Review a copy of the mobile device management policy (MDM).

- Does the MDM allow for employees to use their own device (BYOD)? If so:
 - What are the policies and requirements, especially with processing personal data? If personal devices are used for accessing email, is copying/pasting/downloading blocked?
 - Does LionDive have management profiles on user mobile devices?
 - How are user devices managed?
 - How are employees handling operating system updates (especially for BYOD devices)?

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

92



Exercise: Cloud Services Audit Answer

Vulnerability Management

- Determine the relevant risks to the environment.
- Understand what LionDive's cloud is used for, (for example, storage or financial transactions, or everything?)
- Identify what vulnerability scanning tools LionDive uses for its cloud services, either from their CSP, a third-party, or both.
- Check if scanning tools are being used, how tools are being used, and if the tools and its outputs are reliable.
- Review the scanning output.

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

93



Exercise: Cloud Services Audit Answer

Vulnerability Management

- Assess what LionDive's vulnerability management looks like in its cloud environment.
- Understand if the controls are actually remediating the risk. Some best practices that should be present:
 - Patch management strategy – controlling how data comes into the environment
 - Proactive detection (e.g. penetration testing)
 - Virus detection
- Confirm penetration testing has been completed.
- Verify cloud services are included within an internal patch management process.
- Assess the implementation and management of antimalware in a similar manner as with physical systems.

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

94



Exercise: Cloud Services Audit Answer

Monitoring And Logging

- Ensure that LionDive can access logs as needed.
 - Understand how the logs are being provided and where they are stored.
 - Ensure the logs are consumable (able to be condensed to a usable level; 81,000 logs almost impossible to monitor, but after they have been condensed to 10 based on patterns, they are able to be read).
 - Understand who has access to the logs and what level of access and permissions are configured.
 - Ensure the logs are protected and can be accessed only by approved and authorized personnel.

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

95



Exercise: Cloud Services Audit Answer

Monitoring And Logging

- Ensure the logs **comply with policy**.
- Ensure the logs **inform (communicate with) incident response**.
 - Review the cloud host-based IDS (intrusion detection system) on the compute instances in a similar manner as with physical systems.
 - Review evidence on where information on intrusion detection processes can be reviewed.

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

96



Exercise: Cloud Services Audit Answer

Incident Response

- Verify that an Incident Response Plan exists.
- Understand **LionDive's definition of an incident** that impacts the risk of what's in the cloud. Ask for the definition of the communication escalation path. It can be the same as on premises but understanding the hand-offs is important because the technology can be different in the cloud.
- Evaluate the process **for incident closure/resolution**.

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+--+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

97



Exercise: Cloud Services Audit Answer

Incident Response

- Understand what is in the CSP SLA for the following:
 - Understand **when** a CSP is required to contact LionDive and when the LionDive is required to contact its CSP.
 - Understand **how** incidents are identified.
 - Ensure the right level of precision/prioritization is being applied to communicate the right incidents.
 - Understand the responsibility to mitigate a breach, the level of detail provided, and mechanisms in place that can be leveraged to monitor and evaluate a breach.

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+--+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

98



Exercise: Cloud Services Audit Answer

Business Continuity And Contingency Planning

- Understand the impact of LionDive's cloud services to revenue, life, or death.
- Understand how each service impacts business operations and what the impact would be if it were to cease unexpectedly.
- Observe contingency planning policies, procedures, alternate storage and processing, backup, recovery and reconstitution.
- Distinguish between data loss and continued operations. The different risks are determined for different sets.
 - Specifically, for SaaS, which tends to be more volatile, understand how LionDive has prepared for a scenario where the SaaS provider shuts down.

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

99



Exercise: Cloud Services Audit Answer

Business Continuity And Contingency Planning

- Ensure the Business Continuity Plan has been tested (should be annually).
- Review the LionDive's periodic test of their backup system for CSP services.
 - The cloud allows for snapshots (backups made at a particular point in time) to be produced more easily – what is LionDive's storage/retention period for snapshots? Have the snapshots been encrypted?
- Review the inventory of data backed up to the CSP as off-site backup. Does LionDive have its own separate backup copy?

[Credit: Cloud Audit Academy 100 \(aws.training\) Cloud+Audit+Academy+-+Audit+Considerations.pdf \(d3dp78hv47f71i.cloudfront.net\)](#)

100