**Mussa Ibn Ashraf Al Arafi**

**Student Id: 209139176**

**Course: Cloud Computing**

**York St. John University(London)**

**Question 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **THREAT AND HAZARD ANALYSIS** | | | |
| **Department: Data Entry Unit** | | | |
| **Sr#** | **Threat/Hazard** | **Potential Impacts** | **Mitigation Strategy** |
| **1** | **Earthquake** | Natural disaster, may damage our hardware. | Use Hardware of cloud vendor |
| **2** | **Ransomware Attack** | Hackers encrypt data for ransom, we may lost our data. | For the security of data, we use the storage space provides by cloud vendors |
| **3** | **Malvertising** | Malvertising is a method of injecting harmful code into legitimate internet advertising networks and web sites by hackers. Users are generally sent to dangerous websites or have malware installed on their computers. Even if users do not click on anything to initiate the download, their devices may become infected. | We will use cloud service to avoid this attack |
| **4** | **Insider threat** | An insider threat happens when someone close to a company who have allowed access to its network misuse that access, either purposefully or accidentally, to harm the company's vital data or systems. | Protect data with tight security features provided by the cloud services providers |
| **5** | **Virus** | System may get infected by the virus which may result in loss of data. | Cloud data protection strategies will be followed |

**Question 2**

**Part 1**

1 – Salesforce Cloud

2 – SAP Cloud

**Salesforce Cloud Backups:**

using a restoration solution that was built from the ground up to function within Salesforce. Inside the Salesforce interface, Spanning Backup enables enterprise-grade, automatic backup and recovery. Say bye to human exports and hello to regular, automatic backups and speedy restores for all your crucial data, documents, folders, and analytics with Spanning.

Spanning works in the backdrop, automatically backing up your Salesforce org on a daily basis at the hour you select – and automatically detecting changes in your Salesforce org for backup.

You may execute a manually backup from Spanning in your Salesforce setup at any moment, on-screen, which is handy before significant imports or new modifications.

Check the status about your latest backups — with recorded counts of modifications for your most essential item types — and Salesforce API use on your customized Spanning dashboard. Chatter postings and email can be used to get backup and restore alerts.

For an irreversible, thorough history of every activity taken by any user inside Spanning, utilize the audit log. For further information, like error reporting and help, look into any backup or restoration.

**SAP Cloud Backups:**

SAP uses backup mechanisms and other safeguards to guarantee that business-critical systems can be recovered quickly when they are needed. SAP HANA provides complete capability for backing up your database and ensuring that it can be retrieved quickly and with little downtime. The recovery point objective (RPO) is 15 minutes or less.

The SAP Business Technology Platform's encryption features are used to encode backups. Backups are duplicated across several network segments within the same area.

Backups are kept for a period of 14 days. This indicates that over the next 14 days, an instance can be retrieved.

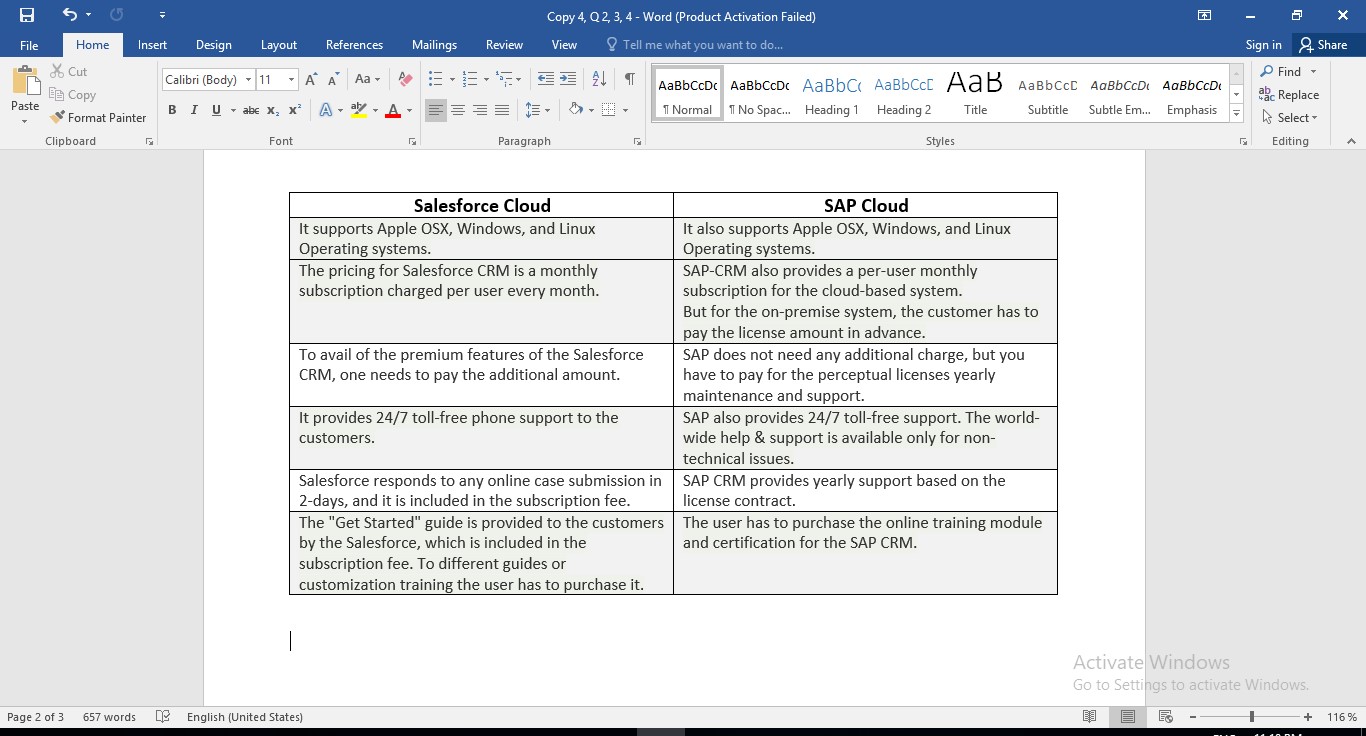
A typical catastrophe recovery solution is included in the SAP BTP Neo environment. It works by restoring data from backups kept in a disaster recovery site. All data saved in the Data Management services and the Document service on SAP BTP is included in the backups.

A disaster's scale is unforeseeable. This might mean that a data center cannot be recovered in a reasonable amount of time and that additional capacity must be established up elsewhere. This may necessitate the buy and installation of new hardware. As a result, we are unable to provide any definite recovery timescales.

The SAP BTP Enhanced Disaster Recovery solution seeks to reduce recovery time by providing asynchronous data replication to a distant disaster recovery location.

**Part 2**

**Comparison of Salesforce Cloud and SAP Cloud:**



**Salesforce Pricing:**

Salesforce can set you back roughly $1,500 per year if you require a CRM solution for all 5 users. Getting promoted to the Lightning Professional tier for a small firm with ten users will cost around $9,000 annually.

**SAP Pricing:**

Backups from your databases are available to download and store to your internal memory on a daily basis rather than monthly. Cloudiax backs up your databases once a day and keeps them for 1 month. At no extra expense, we give you with one of these backups to download once a month. The monthly price of advance backup is 89$ per environment.

Data on Salesforce and SAP is portable to other cloud services providers.

**Question 3**

**Part 1**

Data is organized and saved in a database in the context of an ERP like SAP. This data is then segregated and secured by many levels of security, all wrapped in multiple lines of code that enforces the adherence to a certain data model.

Special tools (modules, functions, and classes) are designed to allow particular operations on this data model in read or write mode in order to interact with it. APIs are the usual name for these tools. APIs are used to communicate with internal data in most new generation apps and ERPs.

SFAPI: SuccessFactors Data API is the acronym for Performance review Application Programming Interface. It's a SOAP Web Service that allows you to import and export data into and out of your Performance review instance. It supports CRUD (Create, Read, Update, Delete) activities for accessing data, and also meta-data activities for data retrieval at runtime. SFObjects, which are similar in concept to database tables, are used to display data. You may list the SFObjects accessible to the API and define the attributes of these entities utilizing meta-data operations. You may query or change data using the CRUD methods.

**Part 2**

While SDLC was designed to save money while meeting corporate objectives, it actually seemed to have the opposite impact in a few cases. Firms that use on-site infrastructure installations may have to wait years for updates, resulting in poor application performance. Cloud software development and deployment is a completely different story. Because CDLC is speedier, it is more sensitive to the ebb and flow of company requirements.

A new web-based, scalable, and distributed service paradigm is also presented by CDLC. The National Institute of Standards and Technology (NIST) has a fantastic explanation that many will appreciate: Cloud computing is a means of offering on-demand system demand access to a shared of customizable computational resources that may be quickly given and supplied with no administration overhead or network operator contact.

The most notable distinctions between the SDLC and the CDLC are the development and launch stages.

Once it arrives to the CDLC's development stage, if development affects IaaS as an infrastructure foundation, this phase is considerably enhanced. The fact that independent software vendors will not have to invest in substantial infrastructure for development, nor will they have to manage or maintain such infrastructure, is a huge bonus.

**Part 3**

2 components of cloud application architecture are:

**Security:**

The backend feature of cloud computing is security, which ensures the safety of data stored in the cloud. The cloud security consists of a diverse combination of rules, technologies, apps, and policies which are used to safeguard IP, data, apps, infrastructure, and cloud computing services.

Awareness of the cloud environment's users, resources, business culture, regulations, security vulnerabilities, and risk management techniques.

Sets out clear baseline automated systems, security settings, and control obligations. For installation across typical use cases, with security protocols, and in international standards on auditing, it's usually standardized and repetitive.

**Internet:**

The Internet serves as the conduit via which the client and server components connect and interact.

Organizations may operate with minimal expenditure and remove on-premises infrastructure by employing a cloud-based solution. Cloud computing is widely used because of its numerous benefits that benefit creativity, innovation, teamwork, security, simplicity of use, and sales.

**Part 4**

A Cloud Directory Platform, for example, is a modern cloud identity management system that offers you to:

* Expand your on-premises Active Directory or LDAP directory towards the cloud.
* Irrespective of location, control your Windows, Linux, and Mac PCs, laptops, and hosts.
* Allows users to connect to apps that employ LDAP or SAML-based authorization.
* Using a cloud RADIUS service, address these risks user access to VPN and Wireless routers.
* GPO-like functionality for distant managing across Mac, Windows, and Linux systems.

In a way, all of these features combine to form a gateway that links users to nearly all of their IT tools, independent of vendor, platform, protocol, or geography, all while allowing administrators to automate the onboard and off-board processes. A contemporary cloud identity management platform may also give full insight into all key activities, which is important in an era where protection, security, and regulation are front of mind.

**Question 4**

**Part 1**

The Health Insurance Portability and Accountability Act of 1996 is known as HIPAA. HIPAA was created with the intention of ensuring health insurance coverage for those who lost their jobs. HIPAA has undergone changes and expanded its scope since its inception in 1996.

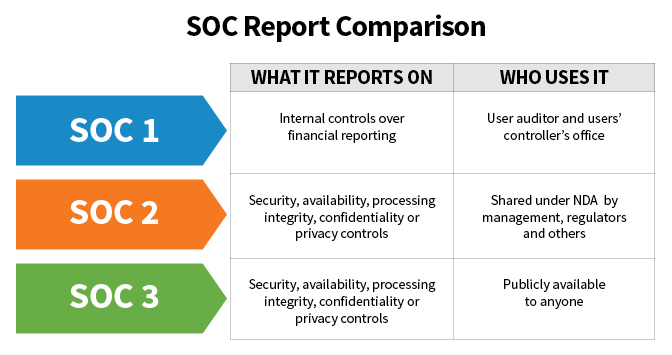
Transactions rule:

This regulation applies to ICD-9, ICD-10, HCPCS, CPT-3, CPT-4, and NDC codes, as well as the transactions and code sets used in HIPAA transactions. To guarantee the health, reliability, and safety of health records and PHI, these codes should be utilized appropriately.

Identifiers rule:

For insurance companies that employ HIPAA-regulated economic and procedural transactions, HIPAA uses three unique identities. The NPI is a ten - digit number used to recognize covered health professionals in every HIPAA administrative and financial transaction; the NHI is an identifier used to identify health care plans and funders under the CMS; and the SUEI is a ten - digit number used to recognize a contractor entity in HIPAA transactions and is deemed the same as the NPI (EIN).

**Part 2**



**Part 3**

**Risk Appetite:**

The key to good risk management is determining how much risk to tolerate. The purpose of risk management, especially enterprise risk management, is to equip leaders and the whole company with the information they need to make business choices based on a risk appetite statement that has been authorized by the executive committee.

A risk appetite statement is a written document that outlines how a company decides to take risks. A risk appetite statement allows a corporation to communicate its risk appetite to internal and external stakeholders. A well-crafted risk appetite statement assists a business in better managing and understanding its risk exposure, allowing leaders to make risk-based choices. A risk appetite statement for the entire firm can be used to steer the risk or compliance program.

In either qualitative or quantitative terms, a risk appetite statement indicates the company's attitude toward risk. Risk-neutral, risk-averse, and risk-seeking are all popular qualitative representations of risk appetite in the public sector. Risk appetite statements are frequently related to operational and financial performance indicators.

**Risk Tolerance:**

An organization that works beyond of its risk tolerance limitations risks jeopardising its risk management strategy, goals, and objectives, and even the entire firm.

To determine its risk tolerance, a firm must first determine the outcome measurements of its primary objectives, such as customer happiness, and then determine the range of outcomes—both above and below the intended outcome—that it is willing to tolerate for each objective.

For example, a company that has set a 92% objective for customer satisfaction may determine that it can live with a range of results between 90 and 97%.

**References:**

* Clark, A., 2021. *Salesforce Backup & Recovery | Spanning Backup*. [online] Spanning. Available at: <https://spanning.com/products/salesforce-backup/> [Accessed 20 December 2021].
* Bravo, D., 2021. *SAP BO Administration - Backup*. [online] Tutorialspoint.com. Available at: <https://www.tutorialspoint.com/sap\_bo\_administration/sap\_bo\_administration\_backup.htm> [Accessed 20 December 2021].
* Adams, J., 2021. *Salesforce Pricing: See Pricing Plans for All Salesforce Products*. [online] Salesforce.com. Available at: <https://www.salesforce.com/editions-pricing/overview/> [Accessed 22 December 2021].
* Simmons, L., 2021. [online] Available at: <https://www.sap.com/products/hana/pricing.html> [Accessed 21 December 2021].
* brown, A., 2021. *Success Factors Integration SFAPI/Odata Tools | SAP Blogs*. [online] Blogs.sap.com. Available at: <https://blogs.sap.com/2015/11/12/success-factors-integration-sfapiodata-tools/> [Accessed 20 December 2021].
* Williamson, A., 2021. [online] Existek.com. Available at: <https://existek.com/blog/sdlc-models/> [Accessed 22 December 2021].
* Miller, D., 2021. *Crash Course: What Is Identity Management? - JumpCloud*. [online] JumpCloud. Available at: <https://jumpcloud.com/blog/what-is-identity-management> [Accessed 23 December 2021].
* Morris, C., 2021. *HIPAA for Providers | HealthIT.gov*. [online] Healthit.gov. Available at: <https://www.healthit.gov/topic/hipaa-providers> [Accessed 21 December 2021].
* Pretorius, D., 2021. *SOC 2 – The SSAE 18 Reporting Standard – SOC 1 – SOC 2 – SOC 3 (Formerly SSAE 16)*. [online] The SSAE 18 Reporting Standard - SOC 1 - SOC 2 - SOC 3 (Formerly SSAE 16). Available at: <https://www.ssae-16.com/faq-category/soc-2/> [Accessed 22 December 2021].
* Zondo, K., 2021. *Managing Safety Risk Tolerance | Magid*. [online] Magidglove.com. Available at: <https://www.magidglove.com/safety-matters/safety-culture/safety-risk-tolerance> [Accessed 21 December 2021].