**DSD 611\_Assessment 2\_Vishwakranti**

**Assessment brief**

Smith Jewellery has traditionally run its own servers and computer systems. The store has four branches in Auckland, Hamilton, Wellington, and Rotorua. They employ 30 full-time permanent staff, and 10 part-time casual staff. They had a dedicated skilful IT person who took care of the software, security and kept everything ticking over. Unfortunately, the IT person left and told them that they had to get their computing into the cloud. That left the staff confused and they hired you to get their computing system up to date.

They want to know the options they have, and what the terminology means. The existing Smith Jewellery software provides management for – stocks, customer profiles, employees, pricing, scheduling, invoicing, POS system (Point of Sales), suppliers, and accounting. Most of their data is static and a mix of structured and unstructured data sets. They would like to eliminate the data storage on their premises but would like to prevent data loss due to natural disasters. The data should be available across all branches when needed and must be accessed by an authorised person. All store information must be stored securely. The current website provides information about the product but doesn’t allow online ordering and purchase. In future, they would like to expand their online business and open more branches in other regions.

Your task is to provide them with **thorough** answers to the following questions. Include hyperlinks to any products you recommend.

**Section 1**- Technical information

* Smith Jewellery is considering storing its data on the internet through a cloud computing provider. Provide the following information related to the cloud data storage: -
* **Identify four types of data/information that will be stored on the cloud provider. [4 marks]**
* Data is a set of values of subjects with respect to **qualitative or quantitative variables.**
* When data is structured and well organised in a given context so as to make it useful, it is called information.
* The main forms of the information are:

- Primary data

- Secondary data

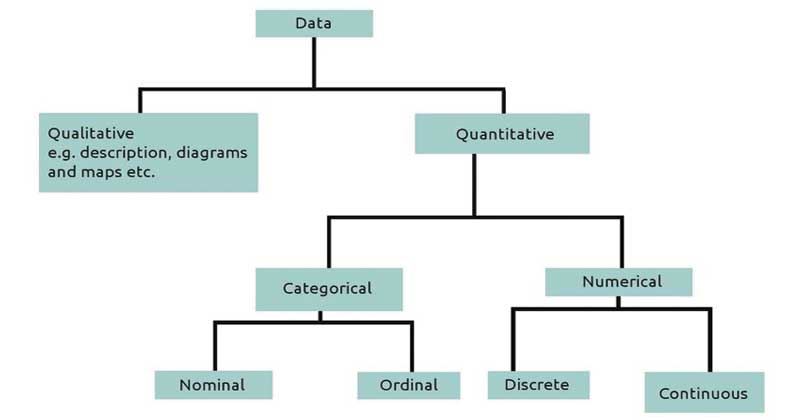
- Cross-sectional data

- Categorical data

- Time series data

- Spatial data

- Ordered data



* As per the **Smiths Jewellers**, they have mixed kind of data in their storage like primary, secondary and cross-sectional data etc. Their existing management provides stocks, customer profiles, employees, pricing, scheduling, invoicing, POS system (Point of Sales), suppliers, and accounting.
* There are four types of cloud data storage: object storage, file storage, and block storage, Optical media storage.
* They (Smiths Jewellers) might have chances to go with private/public cloud system because its ease to manage data storage in a systematic manner.

* **Determine four critical data storage requirements for the store. [4 marks]**

As per the **Smiths jewellers**, their requirements for the store is shown below in briefly.

* **4 Types of Computer Data Storage**
* Computer Data Storage #1: Cloud Storage (Object Storage)
* Computer Data Storage #2: Cloud Backup (File Storage)
* Computer Data Storage #3: USB Flash Drive (Block Storage)
* Computer Data Storage #4: Optical Media Storage

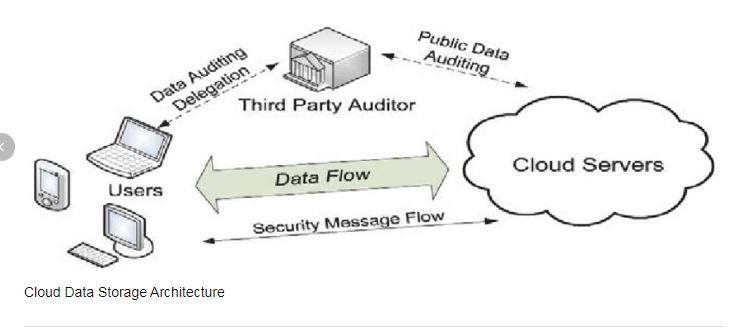
There are several fundamental requirements when considering storing data in the cloud - durability, availability and security.

* During the durability, data stored accurately in every part of the required sections. Natural disasters, human error, or mechanical faults should not results in data loss.
* During the availability, whenever we required our data, it is always available on-demand, but somehow it has differences in production data and archives. The cloud storage will delivering the accurate balance of retrieval times and cost.
* During security, all the data is encrypted while in transit and at rest. Access control and permission work well in the cloud under the premises storage.
* **Data Storage Requirements**
* Establishing Passwords and Accounts.
* Limiting Physical Access to Cardholder Data.
* Storing Data.
* Maintaining Servers.
* Securing Servers.
* Decommissioning Computer Systems and Electronic Media Devices.

Now, the cloud can be the best place to store your business' mission-critical data, providing cost benefit solutions which is easy to manage for any business and very useful for savings.

* **Compare two suitable cloud data storage types (Object storage, File storage and Block Storage) for Smith Jewellery, in your comparison include the characteristics, advantages, and disadvantages. [6 marks] (150- 200 words)**
* As per the requirements of the cloud data storage for **Smiths Jewellers**, they might find that block storage works best for them, if need to store an organized collection of data that can access quickly and if they need highly scalable storage units for relatively unstructured data, that is where object storage shines.
* In block storage model, it has fixed-sized chunks in the media storage which saves data called blocks.
* Block storage is a path for store large number of data in the individual hard drive that is configured by the storage administrator.
* Object storage manages data and links it to associated metadata.
* Types of cloud data storage: object storage, file storage, and block storage. Each offers their own advantages and have their own use cases.

1. [Object Storage](https://aws.amazon.com/what-is-cloud-object-storage/) - Applications developed in the cloud often take advantage of object storage's vast scalability and metadata characteristics.
2. [File Storage](https://aws.amazon.com/what-is-cloud-file-storage/) - Some applications need to access shared files and require a file system. This type of storage is often supported with a Network Attached Storage (NAS) server.
3. Block Storage - Other enterprise applications like databases or ERP systems often require dedicated, low latency storage for each host. This is analogous to direct-attached storage (DAS) or a Storage Area Network (SAN).



**Fig: Cloud Data Storage Architecture**

**Object Storage Characteristics:**

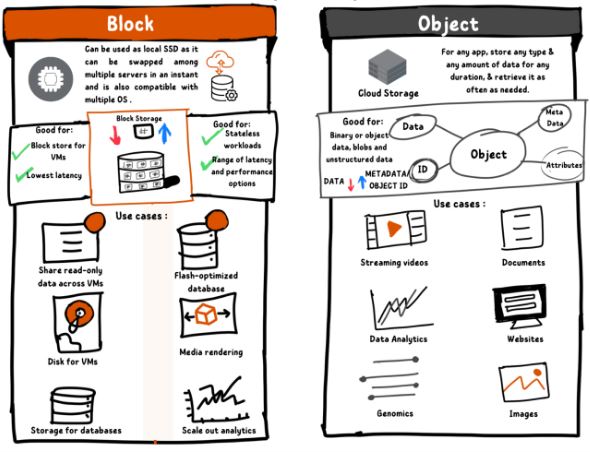
* Storage of unstructured data like multimedia files
* Storage of large data sets
* Storage of large quantities of media assets like video footage as an archive in place of local tape drives

**Object Storage Advantage:**

* Object storage is the famous cloud storage and majority wants to use it widely because, the storage of massive amounts of unstructured data while still maintaining easy data accessibility. It can store greatest amount of data by using flat structure and GUIDs instead of hierarchies’ characteristic of file storage or block storage, object storage allows for infinite scalability.
* By using metadata, it has higher level of accessibility, which is infinitely customizable. Metadata applies a set of labels for your data which can easily be reorganized and scaled, based on different metadata criteria.
* Object storage is very famous for backup and archiving functions. Metadata’s unrestricted nature allows storage administrators to easily implement their own policies for data update, rewrite, edit, delete and make their own strategies regarding data.

**Object Storage Disadvantage:**

* Object storage doesn't allow you to alter just a piece of a data blob, you must read and write an entire object at once.
* You can't use object storage services to back a traditional database, due to the high latency of such services.



**Fig: Difference between Block and Object Storage**

(htt7)

**Block Storage Characteristics:**

* The scale of your data storage needs is unknown or is subject to fluctuation.
* Performance and availability are more important than convenience.

**Block Storage Advantage:**

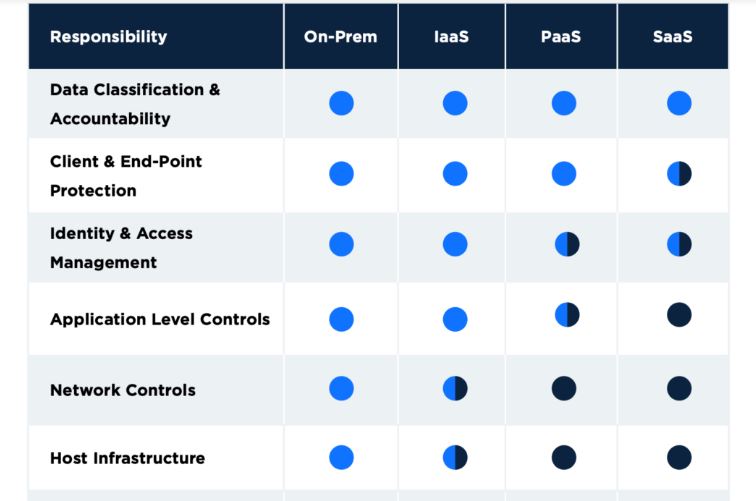
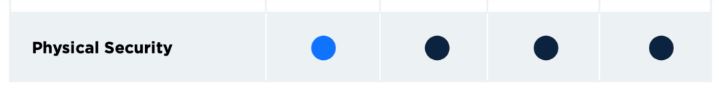
* **Performance Level**: It has rapid input/output data access or the low latency.
* **Flexible**: It has huge capacity that you can add new block of volume easily as per your requirement which is very important for your business growth.
* **Agility**: It can transfer data from one server to another easily. With an iSCSI target path, the data can be pointed to other servers.
* **Filesystem Overhead**: This very important advantage reason is that it removes the read or write activities in the operating system, PHP, Apache, share point etc. are famous for block storage.
* This method has almost eliminated the IO bottleneck issues, as the system do not need to write the data twice during the operations.
* **Bootable**: operating systems can be used to boot directly from the block storage that is presented through storage area networks (SAN). We need a physical or virtual server with a BIOS capable of SAN boot.
* **Permissions Issue**: Access management and data permissions are a bit easy to manage and can be controlled directly by the storage in the blocks or the host of the operating system.
* It is linked to one specified server at a specified time for which the data is to be stored.
* Blocks of data and file systems have very limited metadata about the data chunk of information they are used to store for creation date, owner of the file system, file size.
* We need to pay for the entire block storage space that we have allocated for the data in our system, even though if we are not handling it.
* We can only access it via a running server that is linked at a time.
* It will need a little more hands-on effort to work and configure the object storage, such as file system choices, permissions to the file system, versioning of the files, etc.

**Object Storage Disadvantage:**

* It doesn’t allow to alter a piece of data, must read and write blobs an entire object at once.
* There is no built in data analytics capability.
* Storage is tied to one server at a time.
* **Cloud security is crucial for Smith Jewellery, to evaluate the shared responsibilities in three cloud service models (IaaS, PaaS, and SaaS). You may refer to the *Shared responsibility model* for Cloud Security. [10 marks] (300- 350 words)**
* A shared responsibility model is a cloud security framework and also a shared responsibility between the broader organization and its cloud vendor.
* Cloud security it could be dependent on the different teams within an organization that is the network team, security team, apps team, compliance or infrastructure team.
* Cloud security teams maintains some responsibilities for security as you move applications, data, containers, and workloads to the cloud, parallel provider manages

Some responsibility but not at all.

* Customers are typically also responsible for: Identity Access and Management (IAM) User security and credential and endpoint security.
* This shared responsibility model directly correlates to two recommendations: Cloud providers should clearly document their internal security controls and customer security features so the cloud consumer can make an informed decision. Providers should also properly design and implement those controls.
* Cloud security is a shared responsibility between the provider and the tenant that should be meticulously defined and understood by both parties. Only then can they work together to prevent successful cyber breaches.

**Fig: Shared Responsibility Model**: C:\Users\am\Desktop\SharingModel3_611_2.JPG

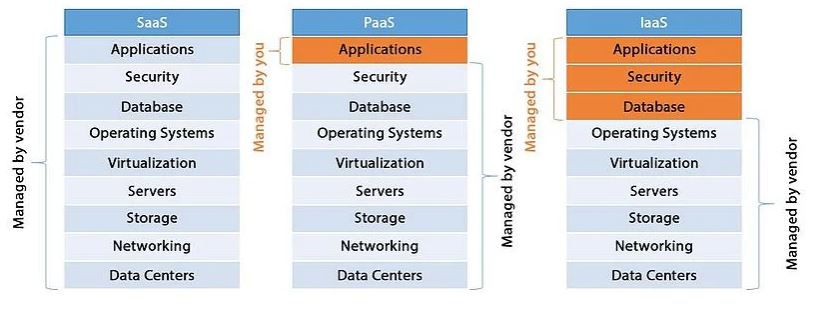
### **Responsibility Breakdown**

There are two ways to think about this responsibility divide. The cloud provider is typically responsible for security “of” the cloud, meaning the cloud infrastructure, typically including security at the storage, compute and network service layers. The enterprise assumes responsibility for security “in” the cloud. This includes applications, data, and services that operate within their managed cloud environment.  However, depending on the cloud infrastructure – private, public or SaaS – responsibility varies between the cloud vendor and organization:

**Private –**In private clouds, enterprises are responsible for all aspects of security for the cloud because it is hosted within their own data canters. This includes the physical network, infrastructure, hypervisor, virtual network, operating systems, firewalls, service configuration, identity and access management, etc.

**Public –**In public cloud, the cloud vendor owns the infrastructure, physical network and hypervisor. The enterprise owns the workloads, apps, virtual network, access to their tenant environment/account, and the data.

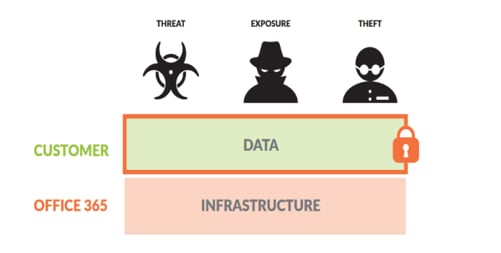
* **SaaS –**SaaS vendors are responsible for the security of their platform, which includes physical security, infrastructure and application security. These vendors do not own the customer data nor assume responsibility for how customers use the applications. As such, the enterprise is responsible for security that would prevent and minimize the risk of malicious data exfiltration, accidental exposure or malware insertion.
* While responsibility for securing data, apps and infrastructure falls more into the hands of the cloud vendor as businesses transition from private cloud to public cloud or SaaS, it’s important to note that ensuring the security of its own data is always the responsibility of the enterprise.



**Fig: Cloud Saas, Paas, Iaas services** (htt9)

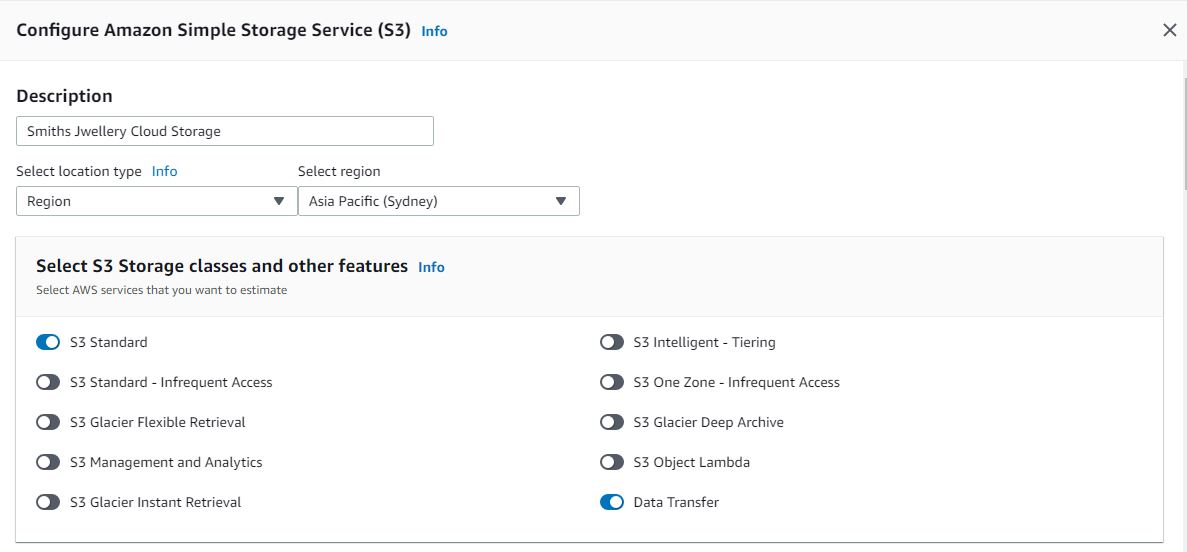
### **Security Measures – Vendor & Enterprise**

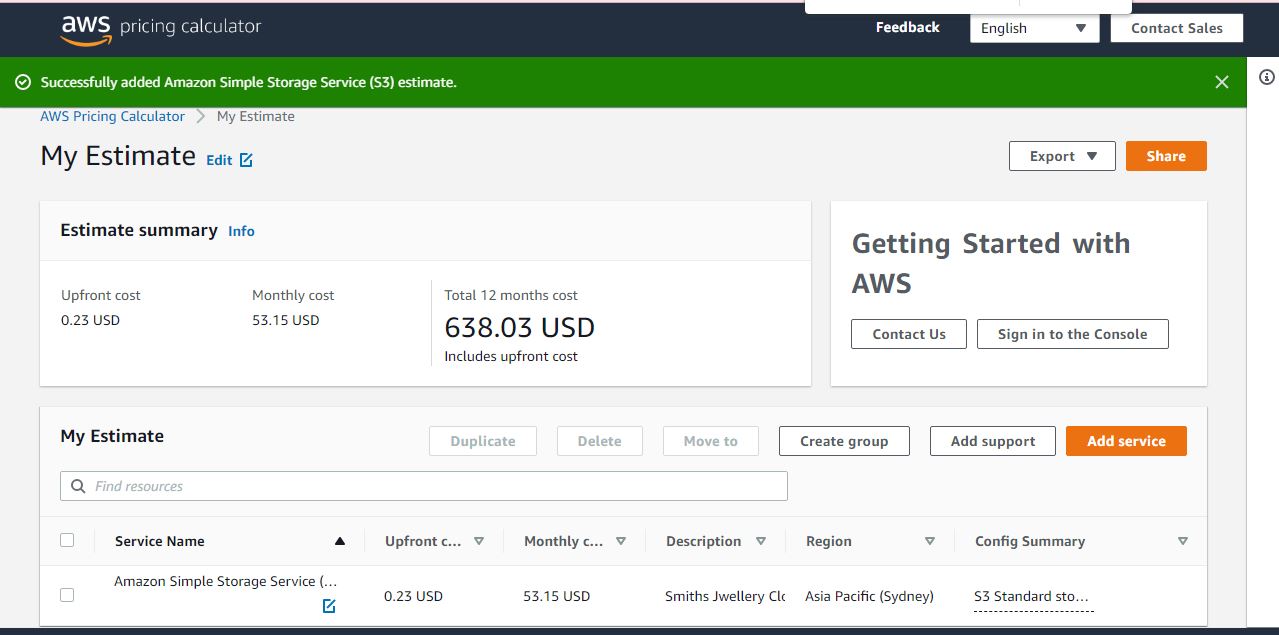
* Because of security and privacy concerns with moving data to the cloud, many cloud and SaaS vendors have focused on ensuring the security of the company’s infrastructure and data. SaaS vendors invest in building a strong defence for their own infrastructure, and they sometimes extend this security to the customer data with basic policy controls.

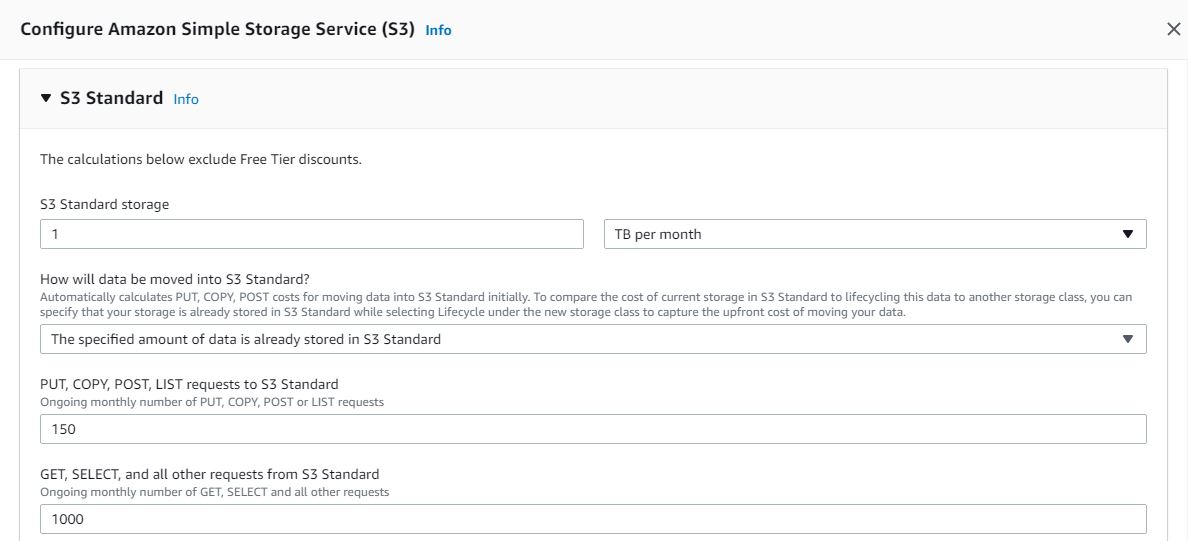
[](https://www.paloaltonetworks.com/blog/wp-content/uploads/2016/12/SaaS_responsibility_1.png)

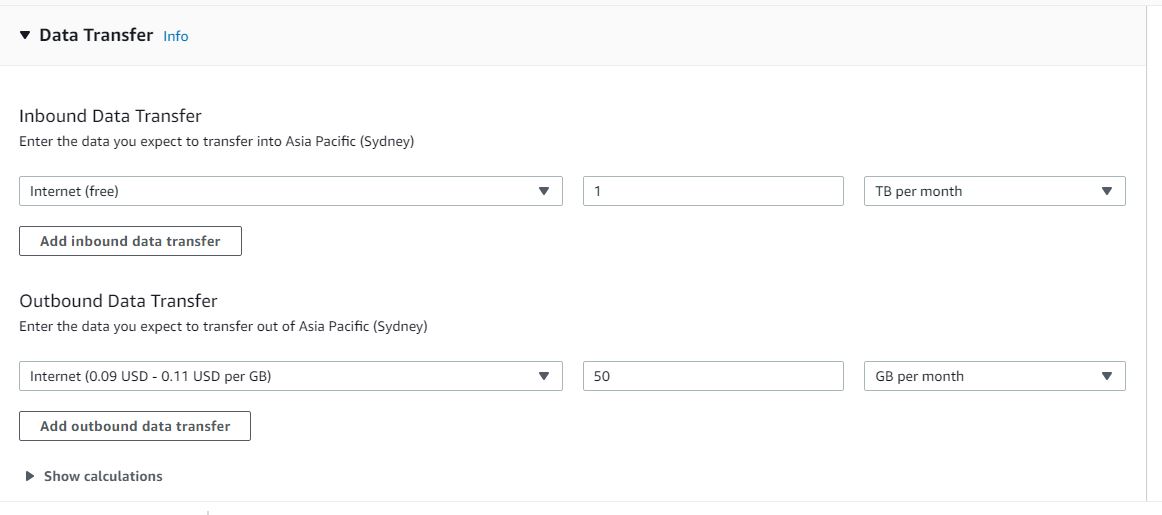
**Fig: Security Measures – Vendor & Enterprise**

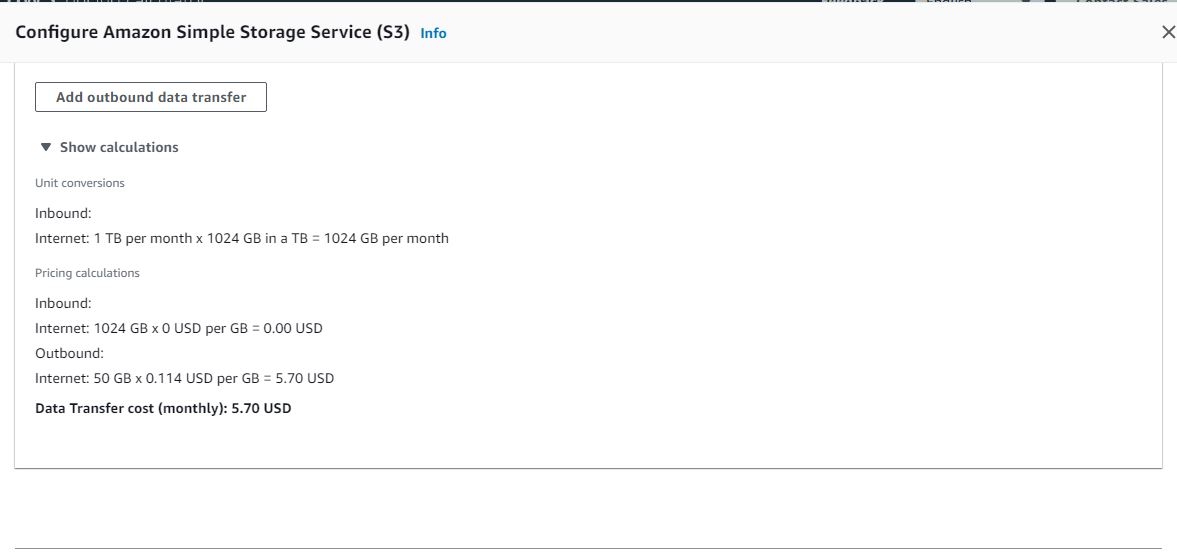
* The IT team’s responsibility is that to fulfil the security gaps and protect the whole company’s data in an appropriate manner. It’s not the Saas vendor’s responsibility.
* To compensate for what cloud vendors do not secure, the companies must have the authority by using the tools about to manage and secure risks to keep data securely.
* In the Saas application, they has to provide how to prevent if the violation occurs and the ability to detect the unknown threats.
* **Recommend one Cloud computing provider with rationale and estimate the cost for the provider. Ensure you include itemised real costs and give them a total package so that they can purchase it immediately. [10 marks] (150- 200 words) (you may add screenshots, please be sure they are clearly visible)**
* Recommended: AWS cloud provider for Smiths Jewellers and providing them total package of cost benefit analysis shown below:



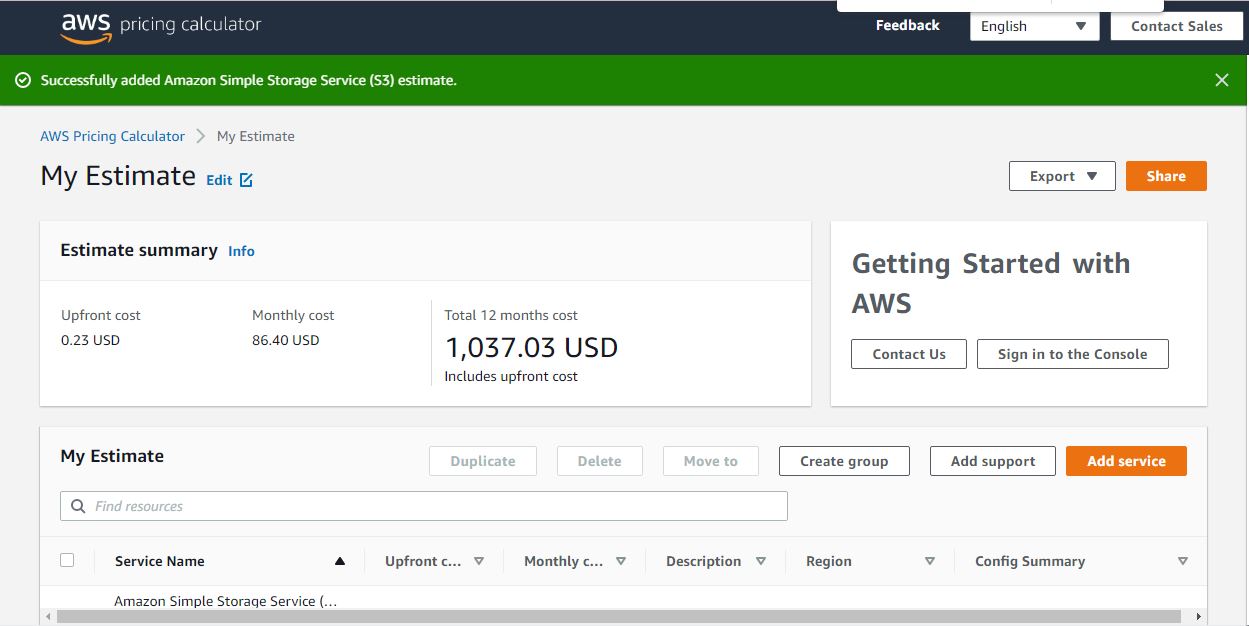








Data Transfer Cost Esimation:



* (htt8)

1. **Smith Jewellery want to upgrade their software, their previous IT employee suggested them to use Cloud Build which provides an integrated CI/CD platform.** 
   1. **Explain how a CI/CD pipeline works and why it would be beneficial for their software development.**

**[6 marks] (150- 200 words)**

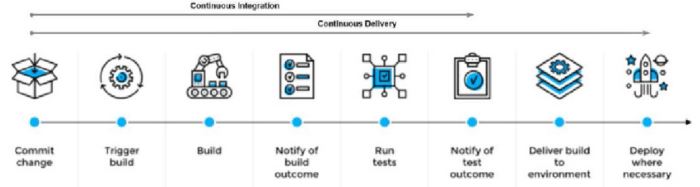
* Continuous Integration (CI) is the process where code updates and changes are collected from a developer or a group of developers and merged with the original source branch. This merger of code with the main branch is called continuous integration.
* [Continuous Delivery (CD)](https://www.opsmx.com/what-is-continuous-delivery/) is a DevOps methodology that enables development teams to deploy changes, such as new features, configuration, bug fixes, and experiments into production safely and quickly in a sustainable manner.
* For a CI/CD pipeline to work, we require a series of sub-processes or stages that need to continuously check and verify the code updates.
* These sub-stages are as follows –

Continuous Integration:

* Code Commit
* Static Code Analysis
* Build
* Test stages/scenarios

Continuous Delivery:

* Publish
* Deploy
* Deployment Testing and Verification
* Monitoring
* Feedback
* Automated pipelines remove manual errors, provide standardized feedback loops to developers, and enable fast product iterations.
* It would be beneficial because you can roll back changes quickly. If any new code changes break the production application, you can immediately return the application to its previous state.



**Fig: Continuous Integration / Continuous Deployment Model**

* Benefits of continuous integration-continuous deployment (CI-CD) Smaller code changes are simpler (more atomic) and have fewer unintended consequences. Fault isolation is simpler and quicker. Mean time to resolution (MTTR) is shorter because of the smaller code changes and quicker fault isolation.
* CI/CD streamlines testing, changes, and deployment of new software’s and new versions, saving a lot of time while delivering a better product. (htt10)
* It is efficient, accurate, provides good quality products, sustainability and scalability are the main benefits of CI/CD which is useful for **Smith Jewellery**.
* (Research Gate, 2021)

**b. Support the use of Cloud Build by providing a detailed justification. [6 marks] (150- 200 words)**

* Cloud Build allows you to build and compile software efficiently across many programming languages which can include Node.Js, Java, and more.
* Many concurrent builds can be run in different pools using different machine types
* The cloud build product can be deployed across a variety of environments including Virtual Machines, Server less components, Kubernetes etc.
* The cloud build can be accessed from a private network which would allow you to control the CI/CD processes from behind any networks.
* It also allows for maintaining data within a preferred geographical location or a specific requirement for a location with residency of data.
* Scans for vulnerabilities can be performed as a part of the build processes.
* The cloud build workflows can be modified to allow for flexibility of certain inputs and parameters.
* Cloud build also allows for server less platforms which provides the ability to scale up or down as required.
* Cloud builds are fast and can be automated for various workflows.
* Many different cloud providers can be used for the CI/CD pipelines based on the product requirements.

**Section 2**- Social, Legal and Ethical information

**5. Research and summarize the following issues related to cloud computing for the Smith Jewellery: -** (Useful resources:- [https://www.digital.govt.nz/dmsdocument/1~cloud-computing-information-securityand-privacy-considerations/html#introduction](https://www.digital.govt.nz/dmsdocument/1~cloud-computing-information-security-and-privacy-considerations/html#introduction) and <https://cloudcode.nz/>)

* 1. **Two social issues (200- 300 words) [8 marks]**
* **Privacy and Confidentiality**
* Privacy about the stored data and information as well as confidentiality is the two social issues occurs in the big businesses and IT sectors.
* It is quite strange that very little attention has been paid to the concept of confidentiality, which must be the core element of privacy.
* Privacy and confidentiality is very similar and works under the near differences such as, privacy comes under the regulations and law as well as confidentiality protecting their industrial norm.
* Privacy rotates around the confidentiality via contract and unbundled term.
* There are number issues regarding privacy so Smith Jeweller must have to review carefully and consider the implications accepting a service provider’s privacy policy under the privacy act.
* Confidentiality, you need to maintain by using unique characteristics to the cloud computing system.
* In the cloud service model, all of the stored information has to maintain confidentially by the service providers but its bit difficult to manage it.
* Smith Jeweller make sure about the privacy act that, clarify with the privacy risks and bind them carefully with the cloud computing system.
* Smith jeweller make sure that, the service provider’s use of personal information clearly set out in its privacy policy.
* Smith jeweller make sure that, the service provider notify its customers if their data is accessed by, or disclosed to, an unauthorised party and also check the providing sufficient information to support cooperation with an investigation by the Privacy Commissioner.
* Smith Jeweller has to check the information about the agency, its staff and/or customers complain to if there is a privacy breach.
  1. **Two ethical issues (200- 300 words) [8 marks]**
* **Ownership and Security**
* Ownership of the premises and their security are the two ethical issues in the IT sectors.
* The ethical issues arise in cloud computing due to privacy concerns surrounding data storage. There are various strategies put in place to protect user information and data in cloud servers.
* Cloud computing is developing as a promising solution to deal with the explosion of computing complexity and data size. One of the  
  main concerns to shift from traditional computing systems to Cloud is ethical consideration and in many cases ethical issues depends on the applications and circumstances.
* There are multiple technological criteria affecting ethical issues  
  in Cloud, such as security; privacy; compliance and performance metrics.
* The main concern has to manage Smith Jewellers is that, the technological criteria which is a set of rules and regulations called Terms & Conditions.
* Terms and conditions(T&C) has to follow by the Smiths Jewellers which is related to the environmental impact that easily forgotten by the stakeholders affected by cloud computing environment.
* Under T&C all of the parties has to pay the penalties in the case of the violation of the rules.
* T&C is an agreement specifying the rights and obligations of users, Cloud  
  providers, and third parties.
* The use of customer data is usually limited to consumer rather than enterprise contracts it is important to determine whether the service provider will use the data for any purpose other than the delivery of the service.
* In the cloud comparison with data in which controls and responsibilities are shared between the application owner and cloud provider, so Smith Jeweller have to be maintain the hardware maintain cost and scalability because it’s under the ownership act.
* Overall T&C, Smith Jeweller has the authority to check and verify everything about the agreement and negotiate it under the company’s lawyer.
* Security is the another unavoidable ethical issue, because there are number of unauthorized access , a hacker or third parties - you may never know  
  who and how your data will be abused, which can lead to several ethical challenges.
  1. **Two legal issues (200- 300 words) [8 marks]**
* **Copyright infringement and Data breaches**
* A legal issue is something that happens that has legal implications and may need the help of a lawyer to sort out.
* Legal standards, regulations, and norms relating to cloud computing are evolving rapidly around the world.
* There are many ways to causing of data breaches such as,
* External Attacks
* Hacking the perimeter (SQL, XSS, and FTP etc.)
* Phishing
* Email spoofing
* Employee Attacks
* Disgruntled employees
* Defecting employees
* Other Internal Attacks
* Trusted business partner
* Non-employee
* Mistakes
* There are some factors for managing risk for data breaches such as,
* Understanding risks
* Patchwork legal framework
* Increasing oversight
* Officer and director responsibilities – Shareholder and consumer suits
* Reputational concerns and consumer trust
* Adopting and documenting security practices
* Security culture
* Cyber insurance
* Good contracts
* Preventing data breaches requires a combination of approaches to manage people, processes, and technologies to implement robust security controls. The security controls that can help you minimize the risk of security breaches. It is impossible to prevent all data breaches that should be know the Smith Jeweller
* Smith Jeweller will need to conduct its own risk management process to settle on a balance between implementing controls to minimize the risk of breaches and the time, effort, and money needed to implement such controls.
* Smith Jeweller could pay legal fees alone if they have got major breaches.
* Smith jeweller has to pay attention about the security breaches that can damage a company’s business and create financial and legal risks.

**Infringement** - Copyright is infringed when a person uses all, or a “substantial part”, of copyright material in one of the ways exclusively reserved to the copyright owner, without the permission of the copyright owner, where no defence or exception to infringement applies.

* A substantial part is any important or distinctive part of the original material. There are no guidelines about the quantity of material or percentage of a work which may be used without permission - it is a matter of fact and degree in each case.
* In some circumstances, infringement of copyright is a criminal offence to which fines and jail terms may apply. The criminal provisions generally apply to commercial piracy.
* As per the above, Smith Jeweller should aware that everything is control under the laws and policy follow it appropriately.

# References

(n.d.). Retrieved from https://www.google.com/search?q=charachteristics%2C+advantage+and+disadvantages+of+file+and+block+cloud+system&oq=charachteristics%2C+advantage+and+disadvantages+of+file+and+block+cloud+system&aqs=chrome..69i57.29749j0j7&sourceid=chrome&ie=UTF-8

(n.d.). Retrieved from https://www.google.com/search?q=iaas+vs+paas+vs+saas+diagram&tbm=isch&ved=2ahUKEwjMkt\_Pg4D6AhWqKbcAHTwdAuMQ2-cCegQIABAA&oq=iaas%2C+paas%2C+diagram&gs\_lcp=CgNpbWcQARgBMgYIABAeEAUyBggAEB4QCDIGCAAQHhAIMgYIABAeEAgyBggAEB4QCDIGCAAQHhAIMgYIABAeEAgyBggAEB4QCDIGC

(n.d.). Retrieved from https://www.google.com/search?q=iaas+vs+paas+vs+saas+diagram&tbm=isch&ved=2ahUKEwjMkt\_Pg4D6AhWqKbcAHTwdAuMQ2-cCegQIABAA&oq=iaas%2C+paas%2C+diagram&gs\_lcp=CgNpbWcQARgBMgYIABAeEAUyBggAEB4QCDIGCAAQHhAIMgYIABAeEAgyBggAEB4QCDIGCAAQHhAIMgYIABAeEAgyBggAEB4QCDIGC

(n.d.). Retrieved from https://calculator.aws/#/addService

(n.d.). Retrieved from https://www.clariontech.com/blog/saas-vs.-paas-vs.-iaas-an-ultimate-guide-on-when-to-use-what

(n.d.). Retrieved from https://www.opsmx.com/blog/what-is-a-ci-cd-pipeline/

Research Gate. (2021, 01). *The Development of a Simulation Model for Assessing the CI/CD Pipeline Quality in the Development of Information Systems Based on a Multi-Agent Approach*. Retrieved from Research Gate: https://www.researchgate.net/figure/Example-of-CI-CD-pipeline\_fig1\_355588293

(Government, n.d.)

(n.d.). Retrieved from https://www.digital.govt.nz/dmsdocument/1~cloud-computing-information-securityand-privacy-considerations/html#introduction and https://cloudcode.nz/ )