<u>Traditional Data Centre to Hybrid Cloud</u>

The Company:

Global Blue (GB) was the first company to introduce the concept of tax-free shopping 40 years ago, tax-free shopping is about refunding the VAT/GST levied in normal stores on the high street to non-resident visitors who will privately export the goods purchased, according to the legislation in the European Union and other countries.

GB has become the top strategic technology and payments partner, enabling merchants to capitalise on the expansion of international buyers, thanks to continuous innovation. GB provides merchants all over the world with dynamic currency conversion, marketing services, point-of-sale technology, retail staff education, and customer intelligence along with tax-free shopping product.

GB completed 35 million Tax Free Shopping transactions worth €18.5 billion in store sales and 31 million Added-Value Payment Solutions transactions worth €4.4 billion in the fiscal year ending March 31, 2019. GB headquartered in Nyon, Switzerland and has over 2,000 employees in 52 countries.

Since August 2020, GB has been listed on the New York Stock Exchange under the ticker symbol "GB." GB recently acquired a leading Software-as-a-Service (SaaS) technology platform that improves the e-commerce returns experience for consumers and streamlines the returns process for retailers all over the world, and in 2020, GB acquired a minority stake in Yocuda, a leading digital receipt generating company. Yocuda enables shops to send customers content-rich, personalised digital receipts while also capturing data for customer insight, management, and engagement. Its technology can also be linked to loyalty programmes for brands. (Globalblue, 2021)

Current IT infrastructure:

As the company began to computerise its processes from paper-based manual processes, it chose the usual route of establishing its own IT infrastructure, as did most emerging businesses at the time. Initially, a decentralised strategy was utilised because the company was spread across various countries and continents, but as the company grew and the demand for efficient and effective management over operations and processes grew, a centralised IT infrastructure became more appealing and cost effective. As a result, due to a variety of factors, including legislative requirements, skill pool availability, public & technology infrastructure standards, and operating costs, two countries from two distinct continents have become IT centres.

Currently, except for a few cloud-based applications and services, most of the technological offering are in-house and provided through company-managed and maintained infrastructure.

Challenges:

Even though the current strategy has worked in the past, the company was forced to make changes to addressing the demands such as the ones listed below

- More and more countries where GB operates are digitalising the way they process transactions and this means that, unlike before almost all activities became real-time operations hence the need for a more reliable service in terms of availability and performance across the globe.

GB have responded to this by making amendment to the existing system or creating plugins that can facilitate the digitalisation, but this has caused issues as any problems with this adjusted transaction flows also caused issued to the established process, hence affecting the whole business. Separating digitalised transaction could been a good solution but the resources and the time required for this process not viable with the current setup.

- The present pandemic has drastically altered the working environment. Almost all activities must be performed remotely, which requires opening access to applications and services in a variety of ways so that employees can work from wherever they are, as well as making changes to applications and services that were not previously accessed in this manner so that they can be shared securely with appropriate controls.

  The company have responded to this mainly by trying to provide remote access via VPN access to the company's network. this may have somewhat addressed the situation, it brings huge security concerns and performance issues.

- acquiring new businesses that are already using cutting-edge technology in their operations, as well as events such as Brexit and other country-level regulatory changes that necessitate swift adaption in order to continue functioning in an efficient and regulated manner.

Currently the newly acquired business are running as separate entity in perspective of IT as merging them by upgrading the existing infrastructure will be huge undertaking and costly

- GB has collected a huge amount of customer and their travel and shopping related data over the years and currently perform some limited analysis to produce reports, but with sufficient resources the collected data can be processed and analysed to produce a comprehensive business intelligent report.

  The company have recently spent lot's resources in creating a data warehouse but still lacks the processing power to exploit the available data to the full and produce valuable information for merchants as well as for its own use.

Overall, changing the current architecture to accommodate increasing requirements has been difficult or inefficient, and even where progress has been made, there is still a lot of concern about security and performance.

Proposed solution: A cloud-based (Hybrid) infrastructure for services and applications.

Cloud-based services and solutions, which were only a tiny application of cloud technology little over a decade ago, are now rapidly developing. These service's global income has risen from a few billions to hundreds of billions today. It is expected to increase by 23.1 percent to $332.3 billion in 2021, up from $270 billion last year. (Gartner, 2021)

Cloud's popularity is clear in the fact that it's used by everyone from huge tech businesses to news publications to government agencies.

Introduction to Cloud computing:

According to the National Institute of Standards and Technology (NIST): "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (NIST Cloud Computing Program)

Cloud model promotes availability and is composed of five essential characteristics: On-demand self-service, Broad network access, Resource pooling, Rapid elasticity and Measured Service.

And there are three service models in cloud:

1. Software as a Service (SaaS): This is a software application delivery model in which cloud service providers host and operate their application over the internet for clients to access and utilise.

2. Platform as a Service (PaaS): This model serves as a foundation for developing and deploying custom applications. There is no need to maintain a database, middleware, operating system, or other software because cloud providers will do so for you.

3. Infrastructure as a Service: This approach provides IT infrastructure, so the user doesn't have to worry about managing the hardware, network, storage, or any other activity maintaining the IT infrastructure.

Here is an illustration of the service model:
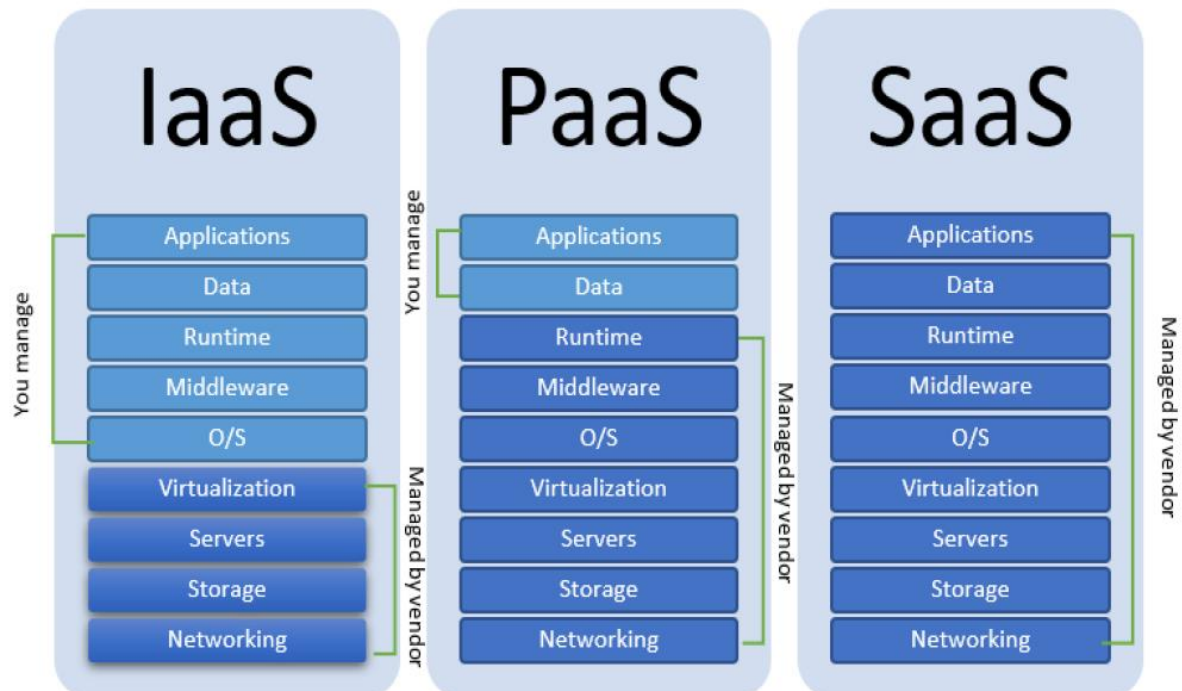
(Wajid H et all.2019)

And four deployment models:

1. Public cloud: A cloud service provider under this paradigm makes cloud infrastructure available over the internet to the general public or organisations.

2. Private cloud: On a technical level, this architecture is identical to the public cloud, except that the resources (applications and storage) are managed by a single entity. The service provider can be another company or a third-party.

3. Community cloud: Because of their reliance on large cloud vendors, some companies are concerned about privacy, efficiency, security, and compliance issues. This strategy is appropriate for firms when cloud infrastructure is shared by multiple organisations with similar needs

4. Hybrid cloud: A hybrid cloud is created by mixing two or more clouds (private, community, or public). It mixes on-premises resources with cloud capability. The fundamental reason for the evolution of this paradigm is that businesses want to keep ownership of their important data. Enterprises have the option of keeping their vital data on their internal network while migrating unimportant data and functions to the cloud. (NIST, Cloud Computing Program)

Why move to cloud:

Benefits:

- Cost: building an on-premises data centre needs a significant upfront investment, as well as ongoing maintenance and specialised personnel to configure and administer the infrastructure. In the cloud, on the other hand, we only pay for what we utilise.

- Rapid deployment: In the cloud, deploying new infrastructure can be done in a matter of hours, whereas on-premises, the same job could take days, if not weeks.

- Scalability: In the cloud, scalability can be automated such that the amount of resources available increases or decreases dependent on demand, allowing the service to operate at peak performance at all times. In the on-premises instance, any scaling will necessitate manual intervention and time, resulting in a failure to meet demand on time, resulting in service interruption or performance difficulties.

- Easy access: While cloud-based services and applications can be accessible from anywhere over the internet, on-premises applications and services may require particular arrangements.

- Disaster recovery: Because information is replicated across multiple locations and regions, cloud-based services will be more reliable and resilient, ensuring quick recovery, while on-premises arrangements will typically lack such a high level of disaster recovery alternatives.

Risks:

- Although cloud computing offers numerous advantages and prospects, there are several concerns to consider before making the switch. Knowing the risks and managing them effectively may ensure data confidentiality, integrity, and availability.

- Reduced Visibility and Control: As data and operations are controlled by the service provider, enterprises lose visibility and control over them when they migrate to the cloud.

- Unauthorized Use: The cloud's on-demand self-service provisioning tools allow employees to provision extra services from the company's cloud platform without permission.

- Multiple Tenants: An attacker can utilise a breach in tenant separation to obtain access to another user's or organization's assets or data by gaining access to one organization's resources through another user's or organization's resources.

- Data Deletion is Incomplete: Consumers have less visibility into where their data is physically kept in the cloud, and they have less ability to verify that their data has been securely deleted.

- Long-term viability: The provider may go out of business or sell to another company if it goes bankrupt.

Why choose a Hybrid cloud:

Given GB's current position and the need to meet future requirements in order to remain competitive in the market and address the evolving needs for making resources available virtually anywhere as they are needed while maintaining control and security, local data centres or public clouds may not be able to meet the needs on their own. A mix of the two would be ideal. As a result, GB should consider deploying a hybrid cloud infrastructure.

To build a hybrid cloud, the current data centre or a portion of it can be simply modified to operate as a private cloud and use IaaS service model from one of the leading public cloud service providers (as IaaS provide the most flexibility for the company).

Enterprises can benefit from hybrid architectures because they provide security, cost savings, flexibility, scalability, and high performance while satisfying business and technical requirements.

Here is an illustration of the hybrid cloud.
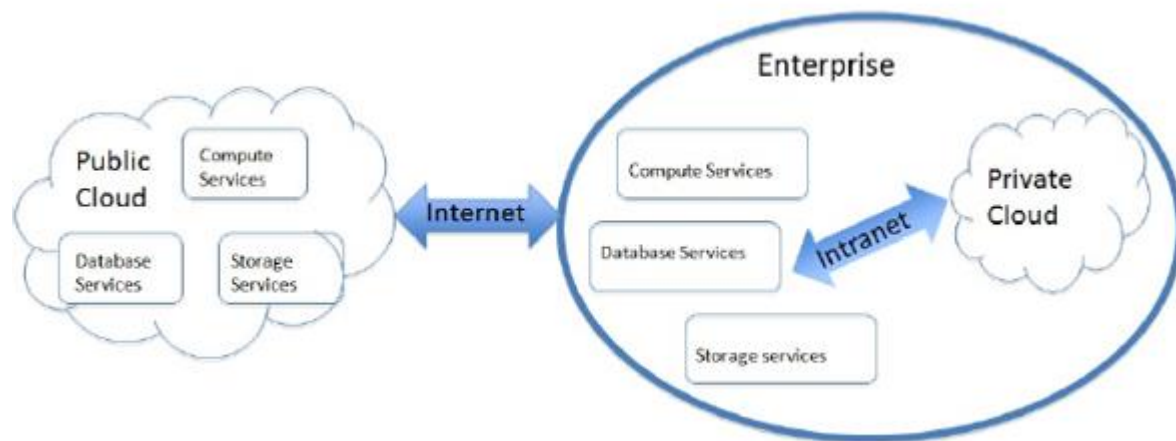
(Koushik A, 2010)

Hybrid cloud model comes with the benefits of a public cloud model but mitigates many risks by allowing a number of different configurations. Here are some examples of such a setup.

Data is one of an organization's most valuable assets and keeping it safe and secure is essential. An enterprise can use a hybrid architecture to keep all important data

and operations on premises while using the public cloud for non-critical applications and services.

This is an example of the arrangement:
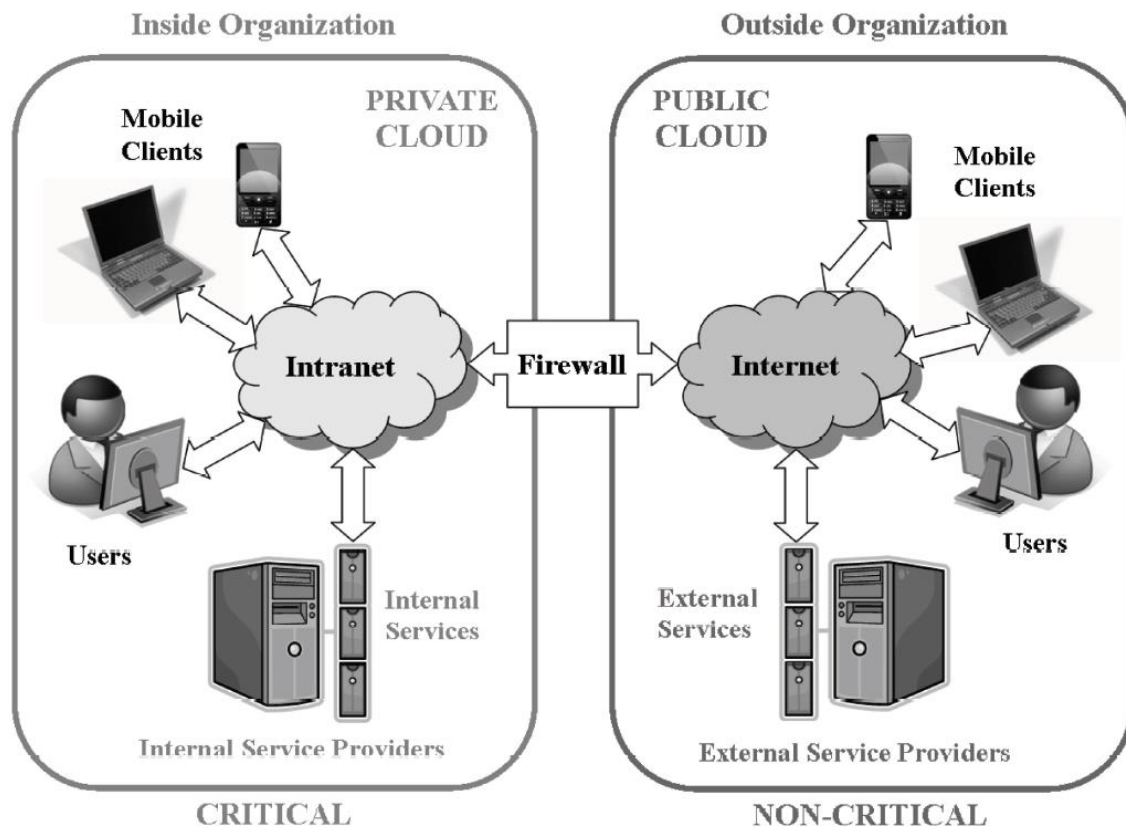
(Peter G et al. 2013)

The majority of enterprise programmes nowadays are multi-tiered and comprise numerous components. A hybrid architecture allows businesses to run their applications partially on-premises and partially in the cloud, reducing the risk of security threats and data and system loss.

VPN (Virtual Private Network) secures access between businesses and cloud services. VPN-based solutions provide businesses complete control over their data.

Use of a Virtual Private Cloud (VPC), such as that offered by Amazon. Enterprises can construct their own virtual cloud within the public cloud, allowing them to host their IT infrastructure on a dedicated subnet. Then, as seen below, a VPN can be built for secure communication.
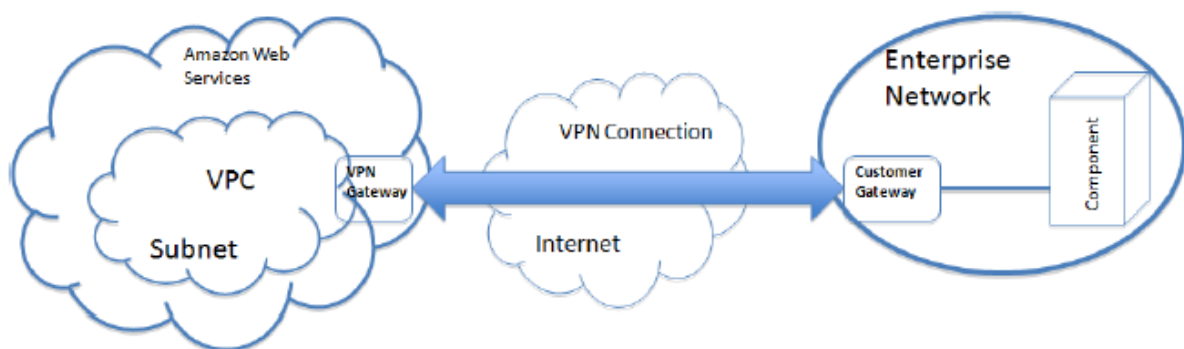
(Koushik A, 2010)

Cloud bridge can be used to create a transparent network with seamless connectivity between businesses and public clouds. OpenCloud Bridge secures and transparently extends the enterprise demilitarised zone (DMZ) into the cloud. Enterprises and the cloud appear to be one network when employing cloud bridge technologies.

In conclusion, a hybrid cloud solution will enable GB to appropriately address current difficulties, as it would provide them with the best of both worlds. i.e., services that are easily extendable and accessible using cutting-edge technology while keeping control and security over the company's most valuable assets. GB will also be able to use new Cloud-based services such as AI as a service (AIaaS) and Quantum Computing as a Service (QCaaS) to analyse the massive amounts of data they've accumulated over the years in order to uncover new trends and insights into their customers' behaviour, giving them a competitive advantage.

References:

Globalblue (2021) about us. Available at: https://www.globalblue.com/corporate/ (Accessed: 24 Jul 2021)

Pankaj A, Rubal W & Er. Satinder A, 2012, ' Cloud Computing Security Issues in Infrastructure as a Service ', International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.

Peter G,Noriaki I,Kôiti H,2013,'Hybrid cloud management: Foundations and Strategies', Review of business and finance studies, Volume 4, Number 1, 2013.

Wajid H, Te-Shun C, Xiaoming L, Patrick A, Omar T, 2019,'Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks', International Journal of Informatics and Communication Technology (IJ-ICT), Vol.8, No.3, December 2019.

Koushik A, 2010,'Security Challenges in Hybrid Cloud Infrastructures', Aalto University, Network Security, T-110.5290, 2010.

Gartner (2021), Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021[Press release], April 21, 2021. Available at: https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021 (Accessed: 24 Jul 2021)

P. Mell and T. Grance, "The NIST definition of cloud computing ," NIST special publication, vol. 800-145, 2011.

NIST Cloud Computing Program Created November 15, 2010, Updated July 9, 2019. Available at: https://csrc.nist.gov/projects/cloud-computing (Accessed: 24 Jul 2021).