# Question 1

## Part A

Cloud computing is the on-demand delivery of applications and services over the internet. It is characterised by three core services: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The industry has been rapidly shifting to cloud computing as the primary means of delivery of applications over recent years, with many large technology companies such as Microsoft, Google, and Amazon providing their services through platforms such as Azure and AWS, with a high degree of success. The company, Trent Solutions Limited (TSL) wishes to move their development operations to the Microsoft Azure PaaS and utilise this as a means of developing their currently on-site application, ‘EasyHR’, into a SaaS. This utilises cloud computing to improve the delivery of the service, based on market trends suggesting a rapid shift from on-site software to SaaS.

The movement to cloud computing can introduce several sources of risk for TSL. Risk is defined as the possibility of loss or injury. This means that there is an uncertain chance of some negative impact or consequence on the project, the organisation, or the people involved. Risks can emerge from a variety of different sources, for example an unprecedented shift in the industry, or the absence of key staff may cause a project to become more unsuccessful than initially identified. Managing risk is a key area of project management and can define whether a project will succeed or fail. There are multiple methods of assessing the impact of a particular risk. Quantitative analysis is the use of decision trees with probability, or Monte Carlo simulations to calculate an objective measure of the likelihood, probability, and impact of a risk. Meanwhile, Qualitative analysis consists of labelling each risk with their relative probability or likelihood of occurrence, and how the risk will impact the project.

One area of risk for TSL when moving to PaaS for their development operations is the lack of staff expertise in this specific area of the field. The company has stated that they sometimes face a challenge in securing technical staff with an ideal mix of deep and broad technical expertise, with good teamworking and communication skills. This suggests that as the company moves to the Azure platform, they may suffer difficulties in acquiring a team that is capable of efficiently utilising it for the purposes of developing their software into a SaaS solution. It can already be identified that the company has many staff who are unfamiliar with cloud computing and the concepts it introduces, such as the. The source of this this risk is staff skills. If the staff don’t have the required skills for using the PaaS, developing any technology will become difficult, and require more time than estimated. The likelihood of this risk is medium, as the company may be able to acquire the correct staff through rigorous recruitment protocols. However, the impact of this risk would be high, as if staff with a lack of technical expertise are acquired, this may cause disruptions throughout the project.

Another area of risk for the company is the lack of managerial skills. It has been stated by TSL that the project manager chosen for the movement to PaaS, while having the technical knowledge required within the field of cloud computing, does not have much experience in project management itself. This could become a risk as the project may become poorly planned and managed, leading to increased costs and time required. Additionally, the selected project manager is working on the movement to PaaS alongside their regular activities within infrastructure engineering, which could cause issue as they may not be fully committed to the project. The source of this risk is Staff Skills and Top Management Commitment. The probability of this risk occurring is high, as it has been stated that the project manager lacks experience in management. The impact of this risk would also be high, as poor management may lead to a failed project that cannot be delivered.

This leads into the third primary risk that has been identified for this project: the unprecedented absence of key staff may further lead to the poor management and delivery of the project. If the project manager has personal issues outside of the workplace that may lead them to not be able to work, the project may fall off schedule and not be executed properly. Especially as the project manager appears to have the most technical expertise with cloud computing. The source of this risk is staff absence. If the project manager becomes absent for long periods of time, the project will go poorly managed, and a primary source of information and expertise in the field will be missing, leading to the development of the project becoming inefficient. The probability of this risk is medium, however the impact of the risk is high, as an unmanaged project can lead to increased costs and time required.

Another risk in a separate area is the unprecedented shift in the market. It has been stated that the market for HCM is very competitive and characterised by frequent disruptions through new solutions and vendors. This suggests that the market is very sensitive to changes in technology, and a new, disruptive technology could emerge that shifts the industry away from cloud computing. The project is primarily justified through a talk that suggests that cloud computing and SaaS will have rapid growth and begin to rival in-premise software within 12 months. A shift in the industry could change that, and customers may no longer be accepting of SaaS solutions. The source of this risk is market changes, and the probability of it occurring is low, as it is unlikely that a new technology will quickly disrupt the entire field of cloud computing. The impact of this risk, however, would be high, as this could easily lead to a failure in the project.

A final risk would be the associated costs of the project. It is possible that the initial estimates of how much the project will cost to conduct wi8ll become inaccurate as the project is planned more thoroughly and formally, which could mean the company, TSL, may not give adequate funding to the project. This means that the project may not be able to be completed effectively, as budget constraints would mean all the requirements may not be able to be implemented. Additionally, the company currently does not know whether they will select the Pay as you go plan or the 12-month plan, for MS Azure. If the Pay as you go plan is selected, it is possible that Microsoft adjust the pricing of Azure in response to competition from other services offered by other companies, such as Amazon Web Services or Google Cloud Platform. This means that the project may unprecedentedly require more money than initially planned to continue. The source of this risk is cost overrun and market changes. The probability of the risk occurring is medium, as it is unknown how the cloud platform market will shift throughout the development of the project. The impact is also medium, as the company may or may not be able to respond adequately through the increase of budget for the project.

## Part B

There are four main responses that a company could have to a risk. Avoidance is the elimination of the specific risk, often through eliminating the root causes. Acceptance is accepting the consequence of a risk should it occur, and not attempting to control it. Transference is the shifting of the consequences of the risk and the responsibility to a 3rd party, Finally, mitigation is the reduction of the impact and severity of a risk by reducing the probability of it occurring.

Risk mitigation is an import aspect of planning a project. If the probability of a risk occurring is reduced, then the potential for project failure is significantly lower. Risks that have a high probability of occurring, or have a high impact, should especially be included in a mitigation strategy, as these risks may be the causes of the failure of a project.

The first risk that was identified was the lack of staff expertise. This risk can be captured through the management of the company and the project. For example, employees with less expertise in the field of cloud computing can be assigned to different sectors of the company, allowing for employees with a greater amount of technical experience to be assigned to the cloud project. Additionally, recruitment of the company can specifically test for individuals with the required expertise through the use of technical interviews and examinations, to ensure the candidates have the skills and experience for cloud-based platforms.

The second risk that was identified was the lack of managerial skills of the project manager of the cloud-based project. This can be captured through the close monitoring and performance of the project, and regular meetings to ensure the project is on schedule and managed correctly. The risk can be mitigated through using an employee with more skills as a project manager to train the new manager and allow shadowing for the gaining of new project management skills and ideas. This would mean the new project manager is able to quickly acquire the experience needed to manage a project effectively.

The third risk that was identified was the unprecedented absence of key individuals within the project, such as project managers and lead developers. This leads to the loss of organisation and key informational sources. This risk can be captured through the regular monitoring of individual employees through meetings and interviews, to assess whether they have any difficulties in their personal lives that may lead to them to become absent from the project. In this case, a suitable replacement can be identified to be substituted for the duration of the absence.

The fourth risk that was identified is an unprecedented shift in the market, leading to the reduction of expected growth in cloud computing. This could be captured through the persistent monitoring of current market trends and keeping up to date with any new disruptive technologies that could change the industry. Analysis of technologies that current competition are utilising should take place, and whether these technologies are likely to have an impact on SaaS in this area of business. This would mean that the TCL is able to make quick, justifiable decisions about the nature of the project, and quickly amend which technology they are using to implement it.

The final risk was the associated costs of the project. This could be mitigated through close monitoring of the performance of the project, and whether it is expected to stay on target or not. Additionally, the analysis of market trends for PaaS pricing, to assess whether the price of the service is likely to rise. This could also be mitigated through the selection of the 12-month plan, which may retain a more stable, fixed value than the pay as you go service.

# Question 3

## Part A

A contract is an important document to be formed between the provider of a service and the organisation that is consuming said service. This is beneficial for both the service provider and the organisation, as it means there will be clarity of what service is exactly being provided and expected, how much is being paid, how changes can be made to the contract, how any disputes will be resolved, and the roles and responsibilities of each party within the contract. This is important as it manages a key aspect of risk within a project, as disagreements between the service provider and the organisation could lead to additional time and funding required by the project to succeed. A guide for how such issues are dealt with can lead to the quick resolution of issues, reducing impact on the project.

Cloud based contracts are extremely beneficial over the on-premise methods. In on-premise contracts, the sourcing lifecycle included much customisation, therefore agreements required long negotiation periods which could often last 6 months or more. With cloud contracts, ready-made solutions that are highly virtualised and standardised exist, with agreements that are standard and available to sign immediately. This greatly accelerates the time required in the crafting and accepting of a contract. Additionally, on-premise contracts are often highly customised and complex, therefore leading to inflexible and lengthy terms. In contrast, cloud-based contracts are simpler, more flexible, and optimised for efficiency. This means that contracts can be made much quicker, and have more flexibility, therefore organisations can make amends to the terms of the contract in response to key factors of the business and the project that may arise at a later date. Finally, on-premise contracts are 1 to 1, meaning they are heavily people and asset based. Conversely, cloud contracts are 1 to many, meaning they are highly standardised and automated. This improves efficiency and fairness of a contract, at the loss of personalisation.

Cloud contracts have several key areas of concern. The contract should define the specific service or services provided, what will be paid for these services and how, how disputes will be resolved between concerned parties such as the service provider or the organisation, what responsibilities each party has, and how the supplier’s performance will be measured.

The service that is being provided should be specified. This includes the accurate description of the service using key terms. An organisation should establish how incidents and problems are managed, and their expectations of the supplier to protect their personal interests. The process for managing change in the contract should be outlined, such as increasing or decreasing the provided services, or suspending and re-enabling them. This is useful in the case of more services than being initially planned required, if the requirements of the project change, or if the organisation wishes to save money as the number of services were overestimated. The organisation should ensure whether they have control over what the supplier provides directly and what is provided through a 3rd party, as this may be pertinent for data security. Finally, any limits or constraints should be identified for the use of the service, so the organisation can ensure they do not break the acceptable use of the provided service, which may lead to disputed between the provider and organisation.

How the organisation pays for the provided services should be clearly stated to avoid any conflicts arising due to miscommunication of payment plans. The basis on which the organisation pays should be contracted, such as fixed fees based on both initial configuration of the services, and variable fees based on consumption of the service over a period of time. The unit pricing should be specified so there is no miscommunication about what the organisation is paying for exactly, for example whether it is volume dependant or usage dependant. Any deadlines should be outlined so the organisation is able to keep track of when it needs to cancel the service or make any changes within the billing cycle, in the case of any changes within the requirements or scope of the project the organisation is undertaking. Finally, a minimum contract period should be identified so the organisation and the service provider both know how long the contract is expected to last, and sudden changes to this cannot be made.

The guidelines for managing disputes should be clearly outlined within the contract. This is an important aspect of the contract for an organisation to protect its interests, as if the organisation disagrees with an aspect of the service provided by the service provider, they are able to quickly and efficiently resolve the conflict without severely affecting their projects. The terms for the termination of the contract should be identified, and the penalty for cancelling the contract outside of these terms. This ensures that the organisation has a period of time to make amends or cancel if they are dissatisfied with the service. The retention of the intellectual property should be defined, as this would mean the work of the organisation has not gone to waste. If this area is ill-defined, the service provider may retain rights over the IP and the organisation would not be able to use it or work on it any longer. Finally, any liability should be defined. This ensures that the organisation and the service provider are not liable for specific issues that may arise through the use of the service.

A final key aspect of contracts is roles and responsibilities. This provides a clear outline of what the cloud provider will be responsible for, and what the customer will be responsible for. This may avoid any issues that arise due to disagreements between the provider and organisation, as a result of miscommunication of what each party within the contract has a responsibility for. Where these responsibilities lie for security and data protection should be outlined, such as how the service provider ensures to protect the data and security of the organisation that is using its’ service. This is important for the organisation as they should strive for the security of their company and their data.

## Part B

The Service Level Agreement (SLA) is a measure of the performance of the supplier. This is the part of the contract which defines exactly what services a service provider will provide, and the required standard for those services. SLAs should outline the expected availability of the service, how reliable it will be, the scalability and serviceability of the service, and how any service credits are triggered and redeemed.

Availability should be specifically defined as the mean time between failures of the service, and the mean time to fix the service. This means that the organisation knows exactly how often to expect any failures, and how long these failures will take to fix. This should also include any scheduled downtime of the service for maintenance purposes, so the organisation can effectively redirect their efforts for the duration of failures or downtime.

The reliability of the service should be defined how many interruptions there may be in the service. This should be outlined as it ensures that the organisation knows how much it can rely on the service being offered, and whether to expect frequent periods of downtime which it can plan and account for, or whether to select a different service provider depending on its needs.

Scalability is the level of which an organisation can expect their usage of the service to be scaled accordingly. The service provider should outline how large loads of data will affect the service, and at which times to expect these loads. This allows the organisation to plan their time effectively around how scalable the service is, so they may assign the correct level of employees to be using it at once.