TMA02

Question 1

There are multiple risks and benefits that should be considered when contemplating migration from a traditional hosting arrangement to the cloud. Major benefits of hosting in the cloud include the elasticity of the resources and infrastructure provided by cloud providers, increased system resilience and reliability due to the virtual nature of the machine instances running in the cloud, and reductions in costs relating to hosting activities. Risks associated with cloud computing are generally concerned with the subject of data, particularly personal data and data protection.

It could be argued that, in the right circumstances, one major benefit of adopting a cloud based infrastructure for hosting purposes is the reduction in the costs associated with hosting activities. This would be of particular benefit to Megamax, as their current IT department is at capacity, meaning that to provide the new portal and order processing application they would have to recruit additional staff members. Cloud hosting would lead to a reduction in time spent by existing staff on deployment activities, such as solving issues, writing deployment code and configuring servers. The cloud takes away the need for these tasks to be carried out in-house, leading to increased productivity of the existing workforce, and the need to employ less additional staff to develop the new and expanded product offerings that Megamax propose. Savings in costs would also be achieved with the removal of the need to house physical machines on-site. Cost reductions here will come from savings on the utilities needed to run and house the machines, as well as savings of the cost of the servers and other network equipment themselves, including spares stored to omit single points of failure in the network. Virtualisation in the cloud means that if a resource fails it can easily be replaced with a new instance, saving the need to have back-up hardware.

Cloud providers are able to offer hosting cheaply, as the virtualisation of the servers means that they are able to utilise the full power of their hosting machines. In-house servers are very often underutilised, and this underutilisation comes at a cost to the business. With the correct architecture in the cloud, Megamax could ensure they are not wasting money on underutilised resources. The virtualisation means that cloud based applications are highly scalable, again leading to cost reductions for the business.

Another monetary consideration of cloud computing is that hosting costs will move from capital expenditure to operational expenditure. This will aid the finances of the business as they will not need to make large payments for any additional hosting infrastructure for the expanding software offerings, with the costs of the cloud hosting just being treated as another utility bill.

When considering cost implications once a move to the cloud has been undertaken, Megamax must ensure that they are not over-provisioning for the applications hosted there. With costs in the cloud calculated by the resources used, it would be easy to spend money that is not necessary by over estimating the demand for the resources. The usage should be monitored so that the correct setup is in place to avoid unnecessary costs. Thankfully cloud providers make this easy with a dashboard view, and so it should be easy for Megamax to monitor resources.

Risks of cloud computing include those surrounding the subject of data protection. Personal data in particular is subject to strict legislation, and as the data that Megamax collect regarding orders could be considered personal data, they must consider this legislation before making decisions regarding cloud hosting. Personal data is data that could be used to identify a living individual, either by itself, or in conjunction with other data that the company may hold. If Megamax outsource some of their IT provisions, it inevitably means that data will have to leave their premises and reside in databases on a cloud provider’s servers. It is the responsibility of Megamax to ensure that the Data Protection Act (DPA) is adhered to, as they are the data controller, and as such are responsible for the protection of the data. The cloud provide will be acting as the data processor on behalf of Megamax, but all responsibility for the following of legislation relating to the data will fall at the feet of Megamax. Cloud providers generally allow the tenant to choose which data centre their physical data resides in, allowing for control over the country, and therefore the legislation that would govern the data that has left their possession. In this way, Megamax will be able to adhere to the DPA by making sure the data is stored within the EEA.

Megamax must also consider that some of the personal data that they collect will be done so outside of the EEA, by their sales operations in North Africa and the Middle East. This will add additional complexity to the data storage solution as Megamax must ensure that they are adhering to the regulations in place within those regions in relation to data processing.

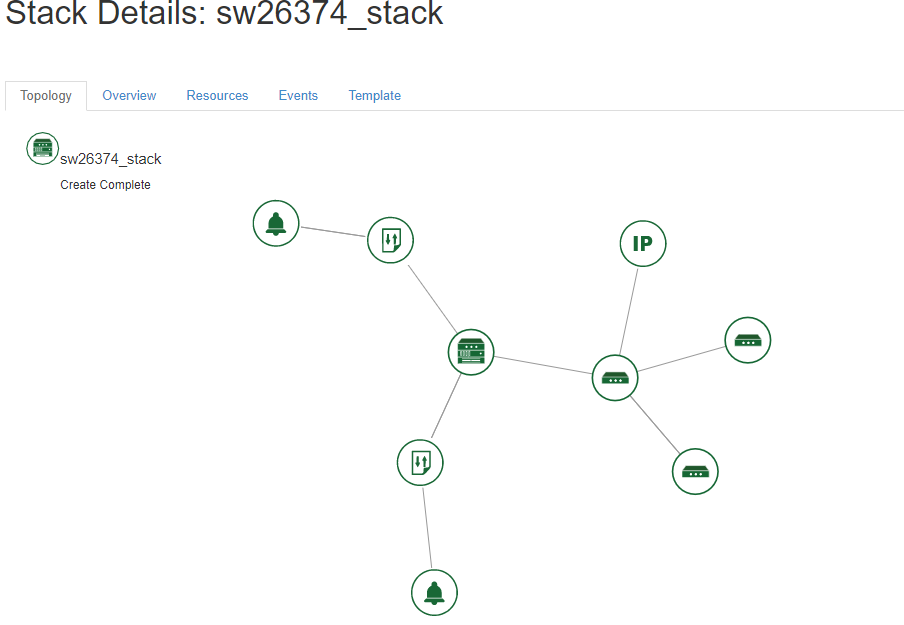
A benefit of moving hosting, and data, to the cloud is that the cloud provider is likely to have very stringent security measures in place, meaning the hosting facilities actually prove more resilient to breaches, and protect the data more effectively than if it were to remain in-house. If Megamax had concerns about data leaving the premises, they may consider using an open source cloud product as opposed to a propriety solution, meaning that it could be hosted in-house, therefore reducing the risks of third party data processing. If the data does leave the premises, then it is the responsibility of Megamax to ensure the data stays protected.

I think it is clear that there are definite benefits and risks that should be considered when deliberating a move to cloud based hosting. It is a major change in practise for any company, and as such Megamax should carry out thorough research around the various points before settling on a cloud hosted solution with a particular provider.

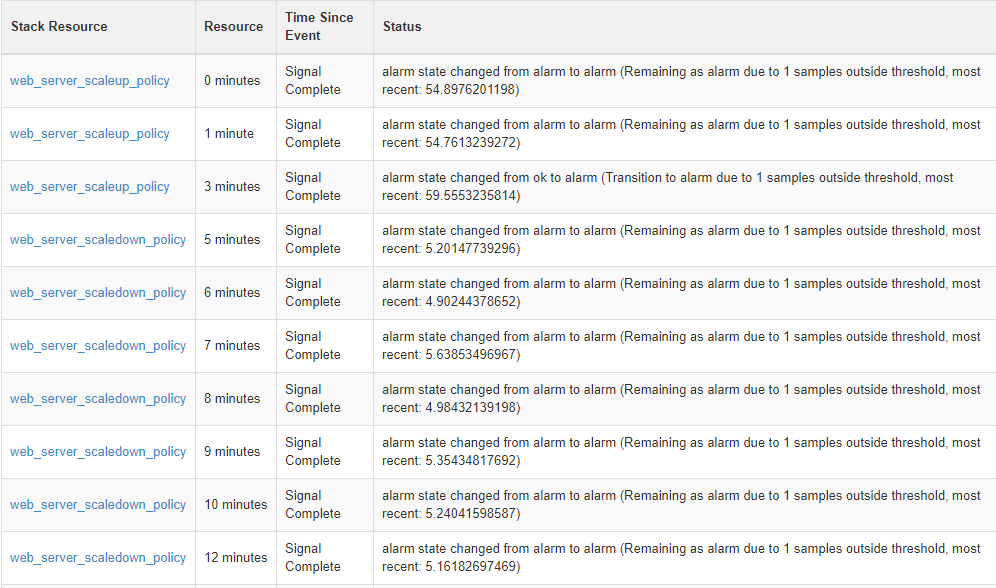
**Word count: 993**

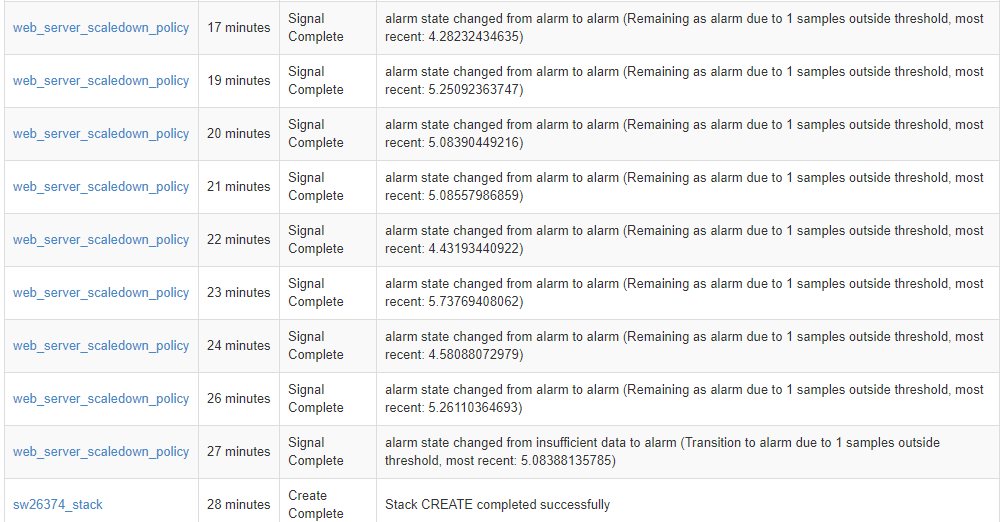
Question 2

a)

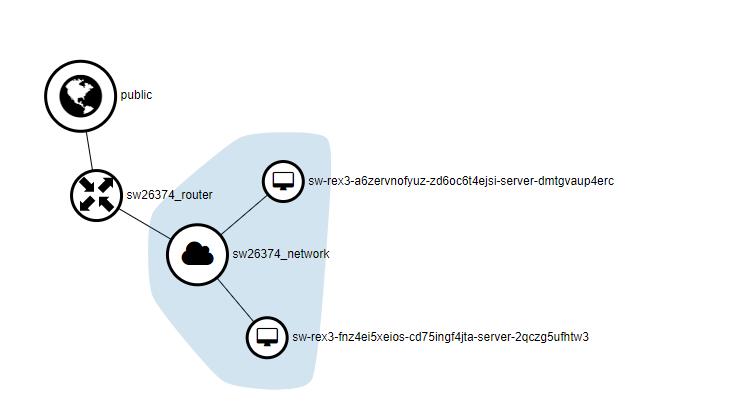


b)

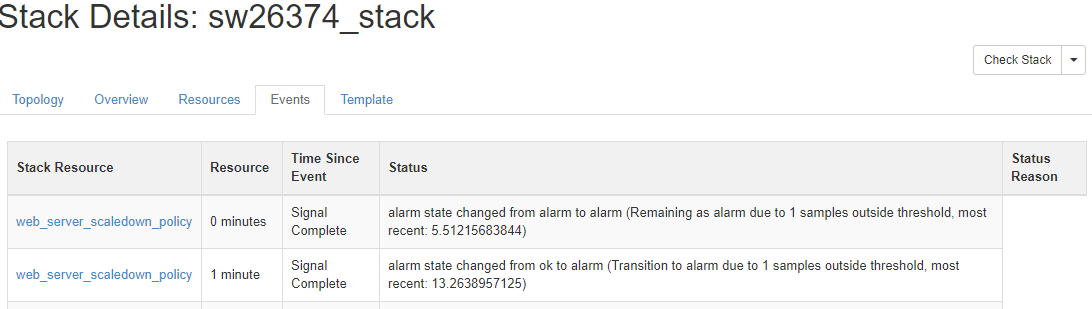




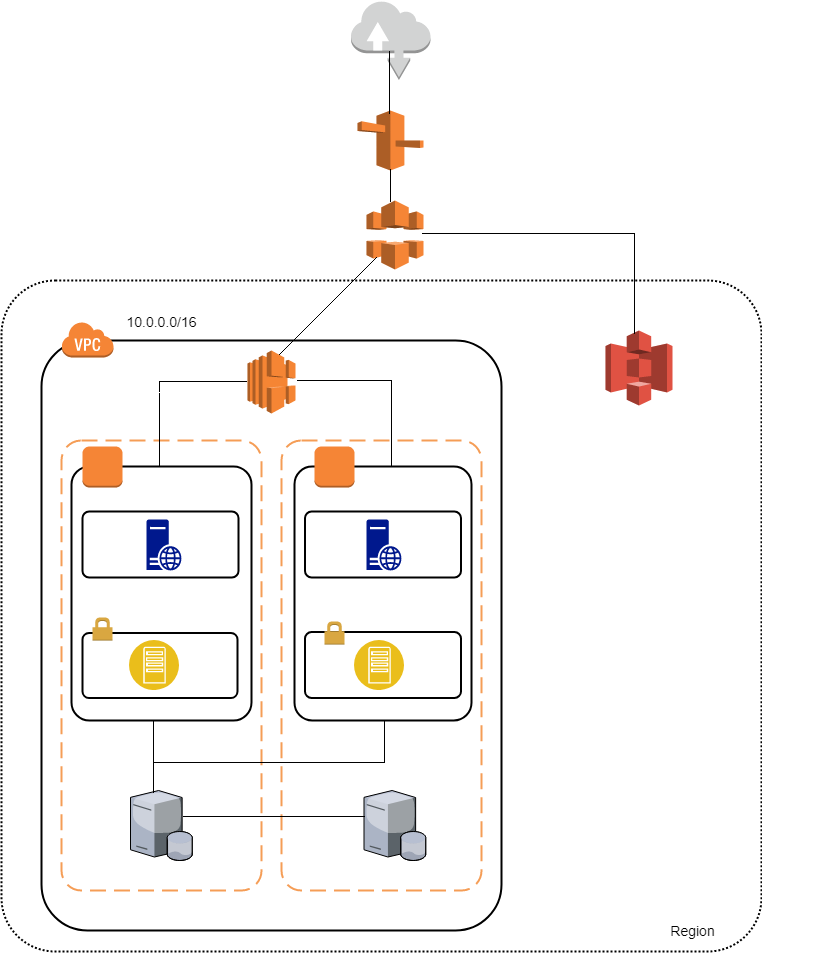
c)



d)



Question 3



Firstly, I have only included a single region for the 3 different business units to all access. This is due to the fact that they should all be using a central database and have the ability to easily access sales information from the other business units, and this would be difficult to achieve using multiple regions specific to each geographical location, as regions are isolated from each other, making it difficult to share data across them.

I have included Amazon Cloudfront and Amazon S3 in the architecture as these would be useful for the file sharing facility of the portal. The storage of static content in S3 and the caching offered by Cloudfront means that the sales team will have shorter response times when retrieving templates and other information from the portal.

The diagram illustrates a Virtual Private Cloud(VPC), which will be private to Megamax as a tenant on the AWS.

I have chosen to include a single EC2 instance in each availability zone to host both the portal and the order processing application. It seems logical that they are hosted on the same machine as they are closely linked in purpose. To allay fears from Megamax that traffic on the order processing site may affect the portal access of their staff, a load balancer has been included on the architecture. This will allow Megamax to set parameters at which the application should horizontally scale, meaning that when the number of requests gets to a point where the application has been slowed down, a new instance can be spun up, and the load shared until demand is reduced again. The load balancer will distribute requests, and therefore load across the instances. Within the EC2 instance there is a private subnet containing an app server that will host the services for the order application and portal, and a public subnet containing a web server that will host the application and portal code.

The diagram illustrates resources spread across two different availability zones within the region. This ensures that if resources in one availability zone fail, instances in another availability zone are able to handle the incoming requests, meaning there will be no down-time of the applications (Amazon, 2018).

**Word count: 367**

**References**

ICO.org (n.d) Cloud Computing Guidance for Organisations [online]. Available at <https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf> (Accessed 03/03/2018)

Froehlich. A (2015) Cloud Computing : 8 hidden costs, *Information Week*, 8th May [Online] Available at <https://www.informationweek.com/cloud/platform-as-a-service/cloud-computing-8-hidden-costs/d/d-id/1321375> (Accessed 05/03/2018)

Amazon (n.d) Regions and Availability Zones [online]. Available at <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>  
(Accessed 04/03/2018)