TMA02

Question 1

There are multiple risks and benefits that should be considered when contemplating migration from a traditional hosting arrangement to the cloud. There are also different degrees to which ‘migrating to the cloud’ can be achieved. Cloud services range from Software as a Service (SaaS) offerings, such as storing files in a cloud storage system, to Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) which involve hosting applications using infrastructure provided by the cloud. This report will consider the factors in utilising a IaaS cloud service.  
 It can be argued that one major benefit of adopting a cloud based infrastructure for hosting applications and websites is the reductions that could be achieved in the costs associated with the hosting activities. This would be a particular benefit for Megamax, as their current IT department is

Risks of cloud computing include those surrounding the subject of data protection. If Megamax outsource some of their IT provisions,

Google cost risks and data protection benefits of the cloud

Several different kinds of costs to be considered, equipment, staffing, intangible.

Could be costs in the way of orders of service provided is unreliable and can’t cope under load, cloud would hopefully solve this.

There are many advantages of moving to the cloud, including …

There are several ways in which consumers can 'move to the cloud'. From using services following the Saas model, such as those offering cloud storage options for documents and collaboration, to

Likely current servers are running at below available capacity, and wasting resources. Money saved from not having to house and maintain own servers. AC, electricity, multiple network components to remove single point of failure.

Cost would depend on the provider chosen (licensed vs OpenSource – research)

As providers are sharing their resources across multiple tenants their hosting options are cheaper as they can spread the costs.

At the end of the day it's down to utilisation. using the cloud means that just as many resources as are required are being paid for, there is no waste, and costs can easily be controlled and monitored.

For MegaMax, where there could be times of high demand, scalability of cloud would be appropriate, and the costs associated with this justified. If constant high workload then physical servers may be more cost efficient/practical.

Companies responsibilities to data protection will not change, as they remain the data controller (reference). Depends on the provider used, OpenStack or other open source would allow data to stay in-house. Proprietary solutions means data will have to go on external servers.

Giving data to a third party if using a cloud provider.

Data regulations must be considered when adopting cloud practises.

Benefits regarding data protection is that the outsourced company

**Privacy**

Concerns about where data is stored, and who has access to it.

If using a proprietary cloud provider then data will likely be stored on one of their servers, leaves your possession.

Using open source then the cloud can be maintained in house

Personal data is that which can be linked to an individual. Users must give consent for data to be collected and stored.

Data controller vs data processor – responsibility if there is a breach.

Data controller – carries data protection responsibility and must exercise control over processing. They determine the purpose for which and manner in which personal data are or are to be processed.

Data processor - any person other than an employee of the data controller who processes the data on behalf of the data controller. Processing means obtaining, recording or storing,

At the end of the day it’s about collaboration, need to be aware of where the responsibilities lie between both parties.

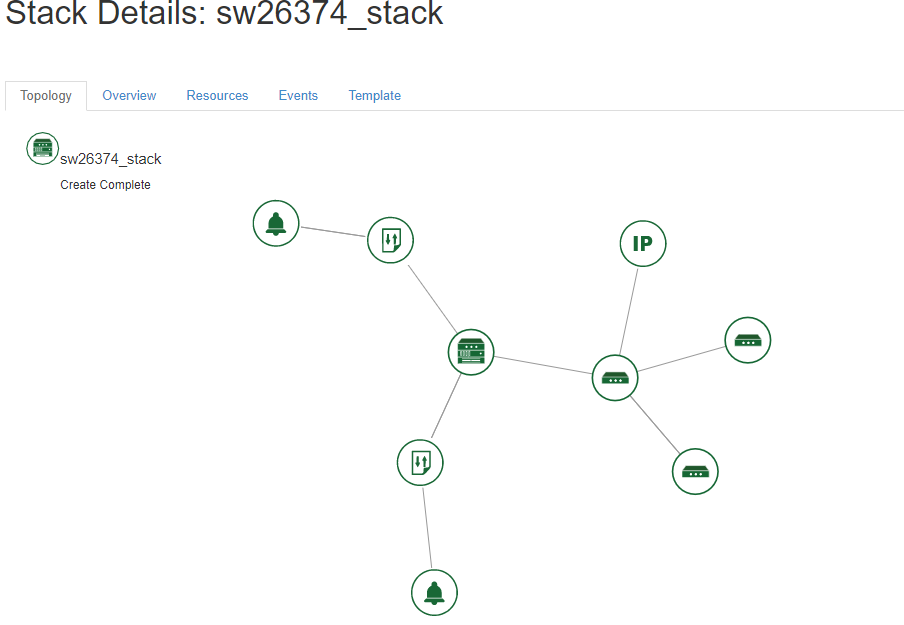
Cloud service provider takes on responsibility of data processor as they are storing data.

Need to choose a cloud provider whose security protocols are sufficient, must read documentation prior to decision making.

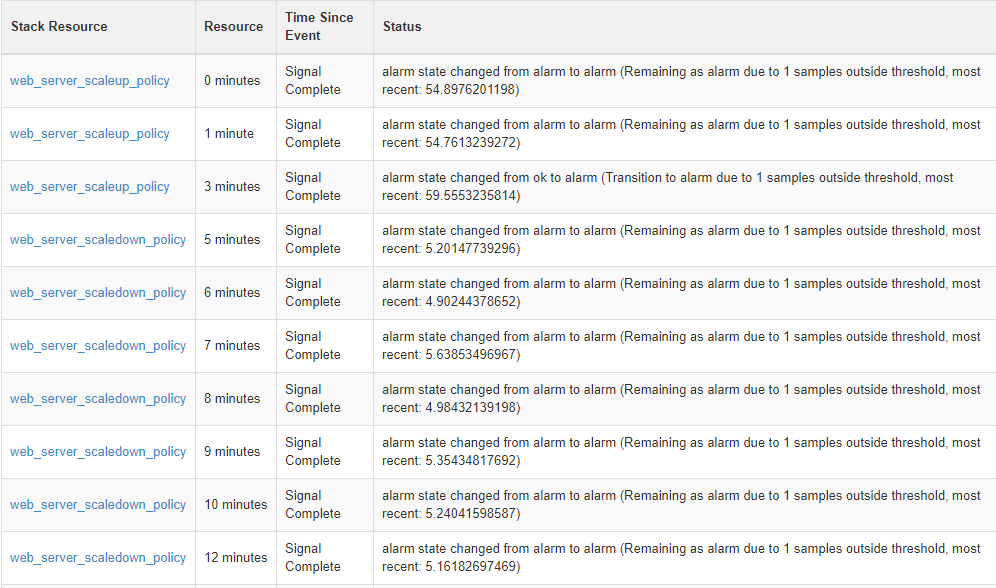
The DPA makes the data controller legally responsible for the processing of personal data it undertakes itself and that is undertaken on its behalf by a data processor. No action can be taken under the DPA against a data processor itself. This is intended to ensure that data controllers put the necessary measures in place to protect their data processing operation from any vulnerability that may arise from their use of a data processor, such as a weakening of security.

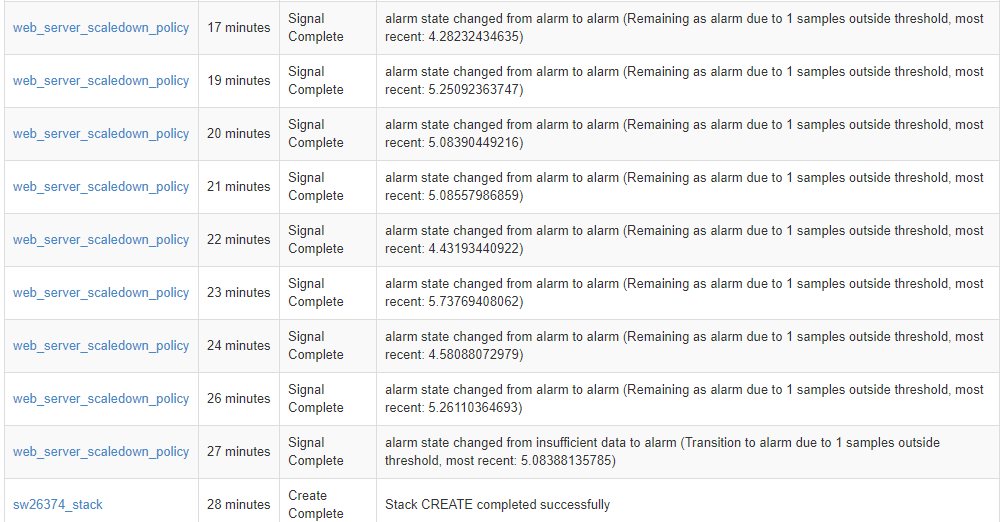
Question 2

a)

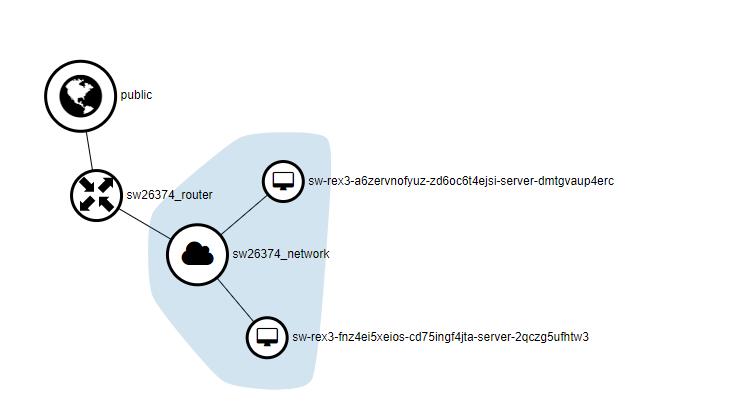


b)

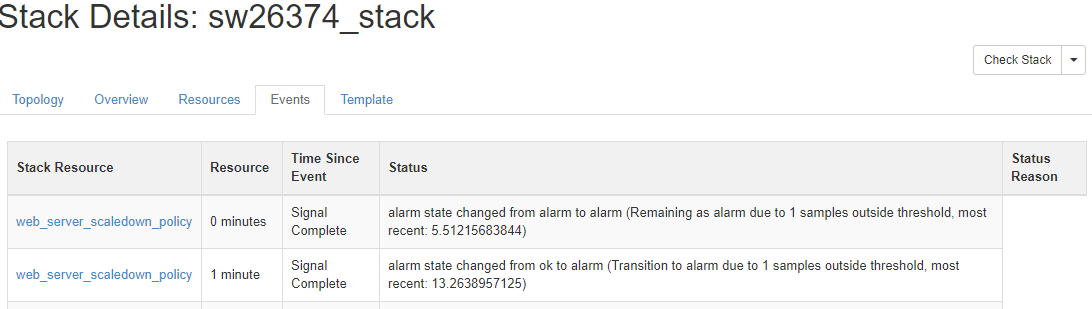




c)



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.  
 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 will aid in the retrieval time of the required files.  
 Another design decision that I have made is to include two availability

<https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf>