**ASSIGNMENT 2 FRONT SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | Unit 16: Cloud Computing | | |
| **Submission date** |  | **Date Received 1st submission** |  |
| **Re-submission Date** |  | **Date Received 2nd submission** |  |
| **Student Name** | Phan Minh Tri | **Student ID** | GCC18015 |
| **Class** | SU-GCC0701-1644 | **Assessor name** | THAI MINH TUAN |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice. | | | |
|  |  | **Student’s signature** | triphan |

**Grading grid**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| P5 | P6 | P7 | P8 | M3 | M4 | D2 | D3 |
|  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **❒ Summative Feedback: ❒ Resubmission Feedback:** | | |
| **Grade:** | **Assessor Signature:** | **Date:** |
| **Signature & Date:** | | |

**ASSIGNMENT 2 BRIEF**

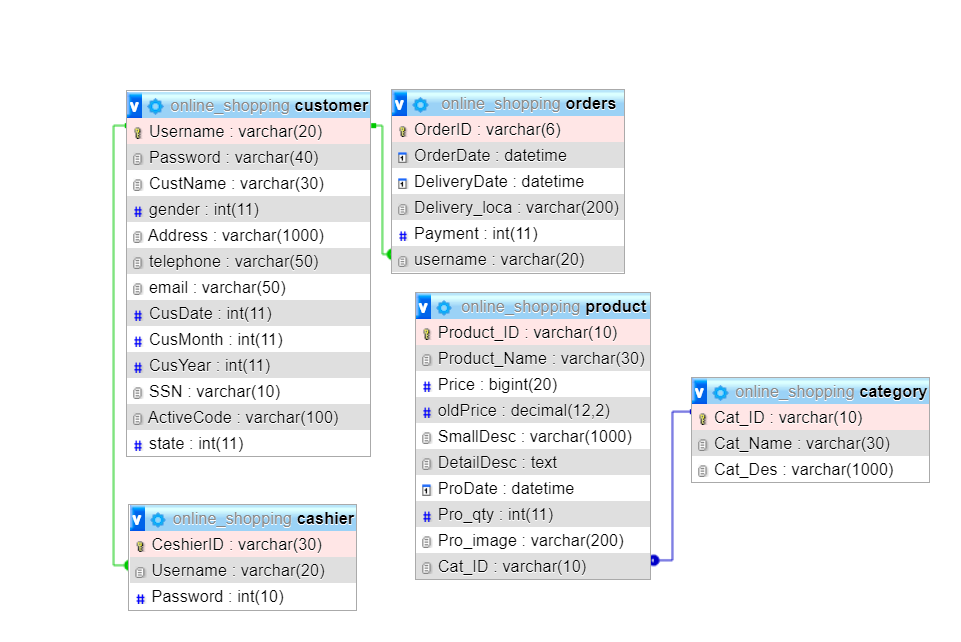
|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number** | Unit 9: Cloud Computing | | |
| **Assignment title** | Cloud’s implementation and security threats | | |
| **Academic Year** | 2019 – 2020 | | |
| **Unit Tutor** |  | | |
| **Issue date** |  | **Submission date** |  |
| **IV name and date** |  | | |

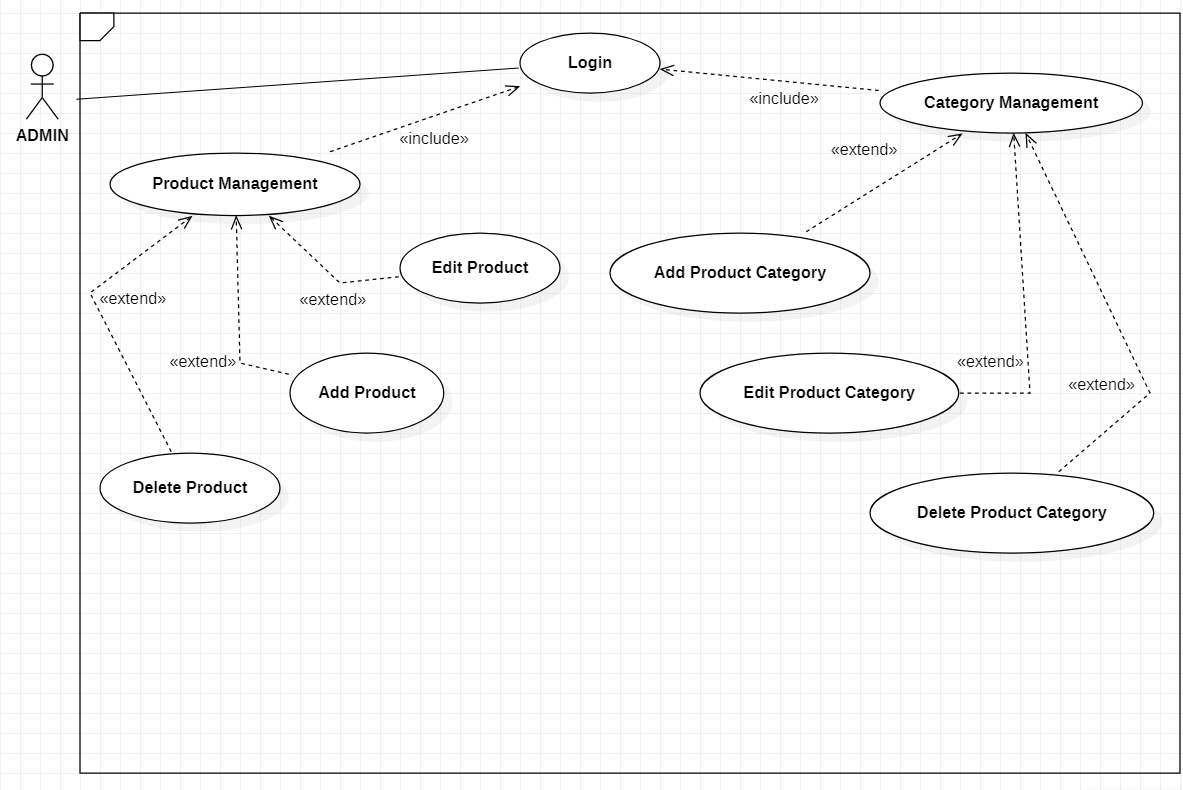
|  |
| --- |
| **Submission Format:** |
| *Format:* A presentation in Power Point format(about 25 pages)  A security manual(in PDF format)  You must use font *Calibri size 12, set number of the pages and use multiple line spacing at 1.3. Margins must be: left: 1.25 cm; right: 1 cm; top: 1 cm and bottom: 1 cm.* The reference follows Harvard referencing system.  *Submission* Students are compulsory to submit the assignment in due date and in a way requested by the Tutors. The form of submission will be a soft copy posted on <http://cms.greenwich.edu.vn/>  *Note:* The Assignment *must* be your own work, and not copied by or from another student or from  books etc. If you use ideas, quotes or data (such as diagrams) from books, journals or other sources, you must reference your sources, using the Harvard style. Make sure that you know how to reference properly, and that understand the guidelines on plagiarism. *If you do not, you definitely get failed* |
| **Unit Learning Outcomes:** |
| **LO3** Develop Cloud Computing solutions using service provider’s frameworks and open source tools.  **LO4** Analyse the technical challenges for cloud applications and assess their risks |
| **Assignment Brief and Guidance:** |
| **Task 1**  Base on the scenario and architecture design in the first assignment provide the implementation. Because of the time constraint of the assignment, the implementation just provides some demo functions of the scenario. The implementation includes two parts:   * A presentation (about 25 pages)   + which shows which functions are implemented   + How to config, deploy and test the services (Web application, Database Server, Source code management, server logs..) using service provider’s frameworks and open source tools.   + Images for the built functions * The source code for the built application   **Task 2**  The table of contents in your security manual (which should be 500–700 words) should be as follows:   1. Analysis of the most common problems of a cloud computing platform. 2. Possible solutions to these problems. 3. Analysis of the most common security issues in the cloud environment. 4. Discussion on how to overcome these issues. 5. Summary. |

|  |  |  |
| --- | --- | --- |
| Learning Outcomes and Assessment Criteria | | |
| Pass | Merit | Distinction |
| **LO3** Develop Cloud Computing solutions using service provider’s frameworks and open source tools | | **D2** Critically discuss how one can overcome these issues and constraints. |
| **P5** Implement a cloud platform using open source tools.  **P6** PConfigure a Cloud Computing platform with a cloud service provider’s framework. | **M3** Discuss the issues and constraints one can face during the development process. |
| **LO4** Analyse the technical challenges for cloud applications and assess their risks | |  |
| **P7** Analyse the most common problems which arise in a Cloud Computing platform and discuss appropriate solutions to these problems.  **P8** Assess the most common security issues in cloud environments. | **M4** Discuss how to overcome these security issues when building a secure cloud platform. | **D3** Critically discuss how an organisation should protect their data when they migrate to a cloud solution. |

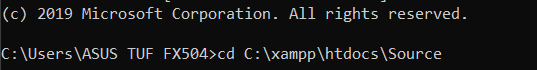
**P5. Implement a cloud platform using open source tools.**

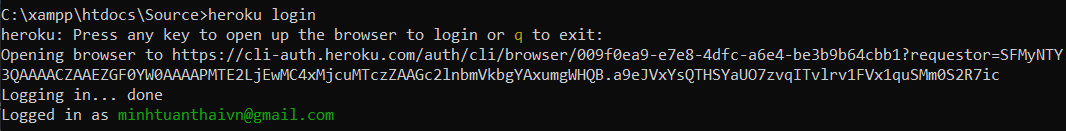
* **Database**



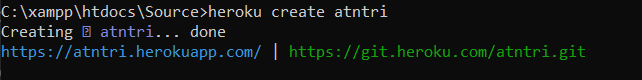
* **Use case Diagram**

**P6. Configure a Cloud Computing platform with a cloud service provider’s framework.**

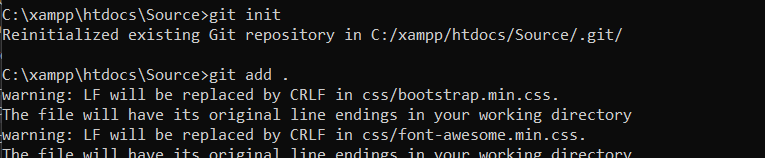
* **Step 1: Choice Source file to**
* **Step 2: Login with Heroku**

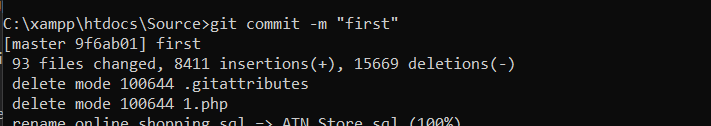
****

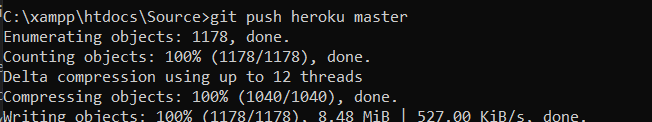
* **Step 3: Create an app on Heroku with name “atntri”**

****

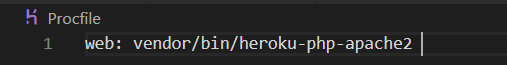
* **Step 4: Deploy my application.**

****

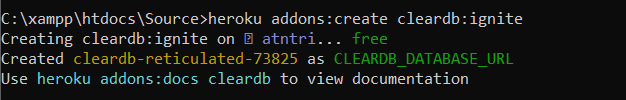
****

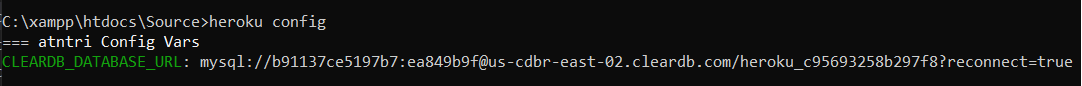
****

* **Step 5: Save as “Procfile” in Visual Code Studio.**

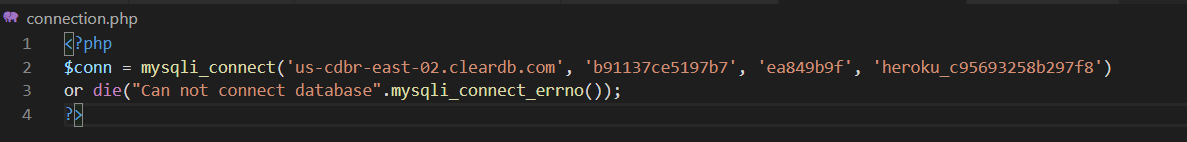


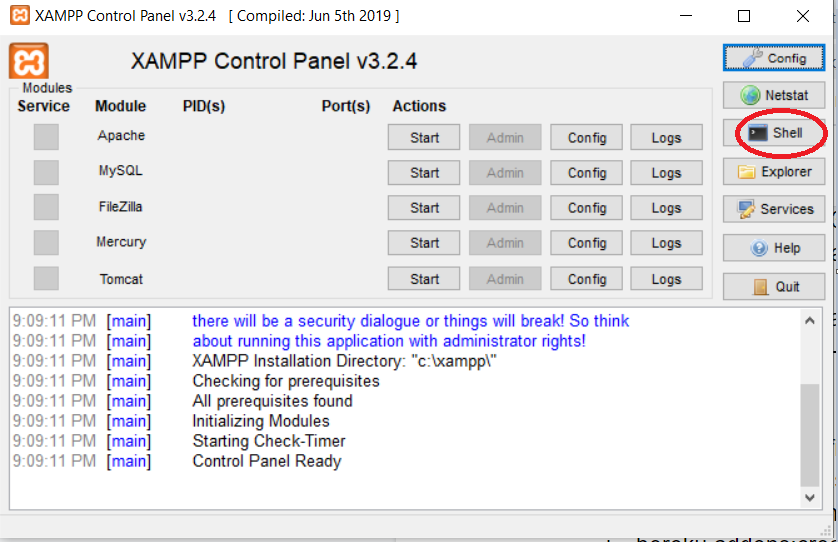
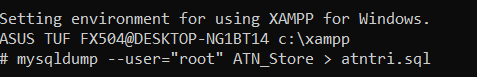
* **Step 6: Database in Heroku:**

****

****

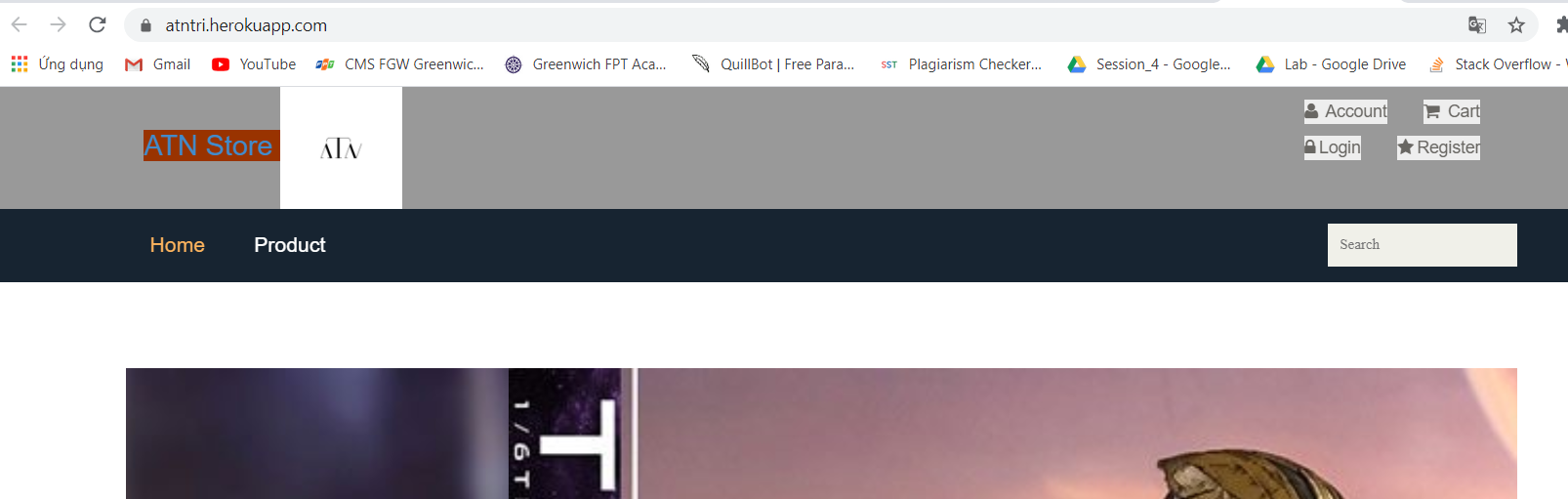
* **Username:** b91137ce5197b7
* **Password:** ea849b9f
* **Host:** us-cdbr-east-02.cleardb.com
* **Database:** heroku\_c95693258b297f8
* **Step 7: Change to “Connection.php” in Visual Code Studio.**

****

* **Step 8: Dump Database:**
* **Go to “Xampp” and click “shell”**
* Export database**:**
* Import database:



* **Step 9: Open we side in “Command Prompt”**
* Enter command: Heroku open

****

* **Link go to the website:** link https://atntri.herokuapp.com/

**P7 Analyse the most common problems which arise in a Cloud Computing platform and discuss appropriate solutions to these problems.**

Cloud computing is used to provide global access to shared resource pools including services, applications, data, servers, and computer networks. It is performed on either a third-party server located in a data center or a cloud owned by a private entity. This makes contrivances that access data more secure and effective, with nominal administration effort.

But there are also many challenges associated with cloud computing and if the company is not prepared to deal with them. Below are common challenges to consider before implementing cloud computing technology. (Anon., n.d.)

* **Data Security**

When we talk about cloud technology's security issues, so much remains unanswered. Many serious threats, such as virus attack website and customers, are the biggest security issues in cloud storage data.

Companies have to think about these issues before they apply cloud computing technology to their company. Because important company information are passed on to a third party, it is crucial to be self-assured about the cloud's manageability and security. Companies need to think about these problems before they apply cloud computing technologies to their company. Since the business passes sensitive company information on to third parties, maintaining peace of mind regarding cloud management and security is vital. (Anon., n.d.)

* **Solution**

The solution given to businesses is to deploy training and certification for their IT team. Besides, cloud providers should release security software and always update and maintain the system so that the tenant does not encounter difficulties.

* **Cost**

Often, developers or other IT workers spin up a cloud instance meant to be used for a short period of time and forget to turn it back off. And many organizations find themselves stymied by the inscrutable cloud pricing schemes that offer multiple opportunities for discounts that organizations might not be utilizing.

For cloud computing to work efficiently you must bear the high bandwidth charges. The company will slash infrastructure costs but they have to pay a considerable amount on the bandwidth. It is not a huge problem for lower implementation costs but is a significant concern for large and complicated applications.

For cloud computing to work efficiently, users have to bear high bandwidth charges. Companies will cut infrastructure costs but they pay a substantial amount for the bandwidth. For smaller applications, cost isn't a big deal, but for large and complex applications it's a major concern. It is really important to have enough bandwidth to transfer complex and expensive data on the network. (Anon., n.d.)

* **Solution:** To minimize the various challenges and complexities by going to the cloud, IT has to change the existing mechanisms of IT governance and control and move them into the cloud. As a result, the position of core IT groups in the cloud has grown in recent years. Central IT plays an increasingly important role in cloud collection and management along with the business units
* **Lack of resources & expertise**

One of the technical problems facing today's enterprises and organizations is the scarcity of resources and expertise. More and more companies, as digital infrastructure continues to grow exponentially, put more workloads in the cloud. Because of those reasons, it is impossible for organizations to keep up with the technologies. The need for skills of IT staff also continuing to grow.

* **Solution**

These problems can be mitigated by further preparation and growth of IT staff training and development. It is necessary to hire more workers with certificates or skills in cloud computing. On the other hand provide training for current employees to help business keep up with technology.

* **Cloud management**

One of the main advantages of cloud computing-speed and ease of implementation of modern computing services-may be a possible drawback. Many organizations lack a view of the "ghost Web" their workers are utilizing, and governance of digital and multi-cloud settings is becoming increasingly challenging.

Experts say some of these cloud infrastructure issues can be alleviated by organizations adopting best practices, including setting and implementing guidelines and policies. And several vendors provide tools for Cloud administration to ease and automate the operation. (Anon., n.d.)

* **Solution**:

Some of these cloud management problems can be alleviated by following best practices, including setting and enforcing standards and policies. And many vendors offer cloud management software to simplify and automate the process. (Anon., n.d.)

**P8. Assess the most common security issues in cloud environments.**

* Privacy policy:

The user data can be accessed with or without authorization from the host business. At any point in time the service provider can access the data on the cloud. They might modify or even erase records, accidentally or intentionally. (Anon., n.d.)

* Compliance:

There are also laws pertaining to data and storage in locations. Users can have to follow costly implementation strategies to conform with the legislation (Federal Information Security Management Act, Health Care Portability and Transparency Act, etc.).

* Security

Cloud-based services include third parties for storage and security. Can one believe that a cloud-based provider can protect and maintain one 's data if one uses their services at a very cheap price for free? They can share information about users with others. Security poses a real threat to cloud. (Anon., n.d.)

* Sustainability:

This topic concerns mitigating the environmental effects of cloud computing. Citing the server's impact on the environmental consequences of cloud computing, countries with favorable environments, such as Finland , Sweden and Switzerland, are seeking to draw cloud storage data centers in places where nature supports natural cooling and green energy is readily available. But other than nature’s favors, would these countries have enough technical infrastructure to sustain the high-end clouds? (Anon., n.d.)

* Misuse:

When offering cloud resources, it can be ascertained that the customer should not purchase cloud storage services for a malicious reason. In 2009, a banking trojan illegally used the popular Amazon service as a source of command and control that provided program updates and malicious guidance to malware-infected PCs.

* **Solution**
* **Deploy Multi-Factor Authentication (MFA)**
* The standard combination of username and password is frequently inadequate to secure user accounts from hackers, and compromised passwords are one of the key ways in which hackers access online business records.
* Once they have user credentials, they can log into all those cloud-based applications and services that users every day to run business.
* Secure users with multifactor authentication-also known as a two-factor authentication-to guarantee that only approved staff is able to log in to cloud applications and access confidential information.
* MFA is one of the simplest and most powerful ways to prevent possible hackers from accessing cloud data. (Anon., n.d.)
* **Manage Your User Access to Improve Cloud Computing Security**
* Manage user rights to boost protection in the Cloud
* Most employees don't need access to every app, every information, or every file.
* Setting the correct authorization level means that each employee can only access or control the software or data they need to do their job.
* Assigning passwords to users not only stops staff from unintentionally modifying documents that they are not supposed to view but also defends the company from hackers who intercept passwords from staff.
* If a phishing email tricked an employee with access to EVERYTHING and accidentally gave their login credentials, so the hacker now has keys to all company records.
* Make sure to partner with a trained IT contractor to help set up the business properly.
* Users will also consider ongoing control of all cloud IT resources by joining up with a Managed Service Provider who can eliminate the customer access and maintenance responsibility directly from the network. (Anon., n.d.)
* **Monitor, Log, and Analyze User Activities With Automated Solutions to Detect Intruders**
* Real-time tracking and user behavior analyze can help organizations spot irregularities other than regular use, such as signing in from an IP or previously unknown computers.
* These anomalous events may suggest a flaw in a company's infrastructure, so detecting them early will deter hackers from creeping and help the organization to address security vulnerabilities until they cause mayhem.
* Get started with automatic 24/7 network management and monitoring and move on to advanced network security solutions such as:
* Intrusion detection and feedback
* Scan and fix security holes
* Endpoint detection and response
* Every company has different requirements for various levels of cybersecurity support, so make sure to get a risk assessment from third parties before making any big investments. (Anon., n.d.)
* **Establish a robust process for protection**
* As staff leaves the company, make sure they no longer have access to the processes, records, consumer information, and intellectual property in the business.
* Because and employee would undoubtedly have access to a range of cloud services and networks, there is a need for a systematized de-authorization mechanism to ensure that access privileges are per employee. When staff leave is removed from the business.
* If this is not feasible internally, do not hesitate to employ this job from a specialist who knows how to set up, execute, and maintain this process properly. (Anon., n.d.)
* **Provide Anti-Phishing Training for Employees on a Regular Basis**
* Hackers can access private information by stealing user credentials from staff using social networking platforms like phishing, spoofing the website, and spying on social networks.
* Providing ongoing training is the best way to prevent employees from falling victim to these scams and compromising sensitive company data.
* The only way to deter staff from falling victim to these scams is to include regular preparation, and to risk confidential company data.
* **General conclusion:**
* The data error rate for cloud services is very low - however the loss of data due to human error is very high. If an employee accidentally deletes data, a hacker will get the employee's account password and corrupt the data or an untruthful employee steals information from his company.
* Companies exposed to rigid laws or concerned about responsibility for missing or damaged data turn to cloud storage solutions.
* The best solution is to speak with a reputable IT consultant to determine which solution is best for the business.
* Following industry best practices in choosing, deploying, providing, and handling cloud resources can help the company make the most of cloud storage, while ensuring a high degree of security.
* Experienced IT experts will help the company develop a robust cloud plan that links all the components together, and also includes continuous monitoring to ensure that the company are safe.
* In general, the cloud is a more cost-effective option, and it's definitely more secure if we take the right precautions.

# References

Anon., n.d. [Online]   
Available at: https://www.datapine.com/blog/cloud-computing-risks-and-challenges/  
[Accessed 4 9 2020].

Anon., n.d. [Online]   
Available at: https://www.techwell.com/techwell-insights/2017/10/6-major-challenges-cloud-computing  
[Accessed 4 9 2020].

Anon., n.d. [Online]   
Available at: https://www.techwell.com/techwell-insights/2017/10/6-major-challenges-cloud-computing  
[Accessed 4 9 2020].

Anon., n.d. [Online]   
Available at: https://www.datamation.com/cloud-computing/top-10-cloud-computing-challenges.html  
[Accessed 4 9 2020].

Anon., n.d. [Online]   
Available at: https://www.datamation.com/cloud-computing/top-10-cloud-computing-challenges.html  
[Accessed 4 9 2020].

Anon., n.d. [Online]   
Available at: https://www.datamation.com/cloud-computing/top-10-cloud-computing-challenges.html  
[Accessed 4 9 2020].

Anon., n.d. [Online]   
Available at: https://www.geeksforgeeks.org/issues-in-cloud-computing/  
[Accessed 4 9 2020].

Anon., n.d. [Online]   
Available at: https://www.geeksforgeeks.org/issues-in-cloud-computing/  
[Accessed 4 9 2020].

Anon., n.d. [Online]   
Available at: https://www.geeksforgeeks.org/issues-in-cloud-computing/  
[Accessed 4 9 2020].

Anon., n.d. [Online]   
Available at: https://www.ntiva.com/blog/6-tips-for-improving-cloud-computing-security  
[Accessed 9 9 2020].

Anon., n.d. [Online]   
Available at: https://www.ntiva.com/blog/6-tips-for-improving-cloud-computing-security  
[Accessed 9 9 2020].

Anon., n.d. [Online]   
Available at: https://www.ntiva.com/blog/6-tips-for-improving-cloud-computing-security  
[Accessed 9 9 2020].

Anon., n.d. [Online]   
Available at: https://www.ntiva.com/blog/6-tips-for-improving-cloud-computing-security  
[Accessed 9 9 2020].