Sa ` `` ` Q



**Data Technician**

|  |
| --- |
|  |

|  |
| --- |
| Name: Anu Chandrasekar |
| Course Date: |
|  |

**Table of contents**

[Day 1: Task 1 3](#_Toc1514505634)

[Day 1: Task 2 3](#_Toc2125927931)

[Day 1: Task 3 4](#_Toc1965065538)

[Day 2: Task 1 5](#_Toc2141651249)

[Day 3: Task 1 9](#_Toc1229522580)

[Day 3: Task 2 10](#_Toc508692763)

[Day 3: Task 3 11](#_Toc1233463339)

[Day 4: Task 1 12](#_Toc1556426903)

[Day 4: Task 2 13](#_Toc214156810)

[1. Scenario Background 13](#_Toc248266112)

[2. Data Laws and Regulations 14](#_Toc1387014804)

[3. Azure Service Recommendations 14](#_Toc1952198484)

[4. Data Types and Data Modelling 14](#_Toc1792190821)

[5. Data Storage Formats and Structures in Azure 14](#_Toc385598743)

[6. Additional Considerations 15](#_Toc561077662)

[Submission Guidelines: 15](#_Toc1001523541)

[Course Notes 17](#_Toc977988415)

[Additional Information 17](#_Toc1081373283)

# Day 1: Task 1

Please research and complete the below questions relating to key concepts of cloud.

Be prepared to discuss the below in the group following this task.

|  |  |
| --- | --- |
| What can cloud computing do for us in the real-world? | Cloud computing in the real world provides businesses and individuals with the ability to access scalable, reliable, and cost-effective computing resources. It supports everything from data storage and software usage to artificial intelligence and big data analytics, transforming industries and everyday life. Its flexibility, accessibility, and efficiency make it a powerful tool for driving innovation and improving productivity. |
| How can it benefit a business? | Cloud computing offers a wide range of benefits for businesses of all sizes. It provides cost savings, scalability, improved collaboration, enhanced security, and access to advanced technologies, among many other advantages. By adopting cloud solutions, businesses can streamline operations, foster innovation, and respond more quickly to market changes, ultimately gaining a competitive advantage. Whether it's a small startup or a large enterprise, the cloud empowers organizations to grow, scale, and thrive in today's fast-paced, technology-driven world. |
| What’s the alternative to cloud computing? | The primary alternative to cloud computing is on-premises computing (also called on-premises IT), where businesses manage their own hardware, software, and infrastructure on their premises or in their data centres. In contrast to cloud computing, where resources and services are hosted by external providers, on-premises solutions require businesses to build and maintain their own IT infrastructure. |
| What cloud providers can we use, what are their features and functions? | There are several major cloud providers in the market today, each offering a range of features and functions tailored to various business needs. The three dominant players in cloud computing are Amazon Web Services **(AWS)**, Microsoft Azure, and Google Cloud Platform **(GCP)**, but there are also other providers like IBM Cloud, Oracle Cloud, and Alibaba Cloud.  **AWS: -**   * **Computer Service** - Scalable virtual servers for running applications. * **Storage Service** - **S3 (Simple Storage Service)**: Scalable storage for objects and backups. * **Networking** - **VPC (Virtual Private Cloud)**: Isolated virtual network for resources. * **Database** - RDS **(Relational Database Service)**: Managed relational databases like MySQL, PostgreSQL, Oracle, SQL Server, etc. * **DynamoDB -** Managed NoSQL database service. * **Redshift**: Data warehousing service. * **Machine Learning & AI -** Sage Maker: Tools for building, training, and deploying machine learning models. * **Security & Identity -** IAM (Identity and Access Management): Manage user access and permissions. * **Analytics**: |

# Day 1: Task 2

Please research the below cloud offerings, explain what they are and examples of use cases.

|  |  |  |
| --- | --- | --- |
| Cloud Offerings | Explain what it is | When / how might you use this service in the real-world? |
| IaaS (Infrastructure as a service) | **IaaS (Infrastructure as a Service)** is a cloud computing model that provides virtualized computing resources over the internet. It offers users access to essential infrastructure components like **servers**, **storage**, **networking**, and **virtual machines (VMs)**, which can be scaled up or down based on demand. Instead of purchasing and maintaining physical hardware, businesses can rent these resources on a pay-as-you-go basis, allowing for cost efficiency and flexibility. | Example: - If we are running a **startup company** that builds a web application, and if we need a robust, scalable infrastructure to host your app. Here's how we can use IaaS in this scenario:  **Step 1: Hosting the Web Application**  You decide to use AWS EC2 (Elastic Compute Cloud) to host your web application. You can choose from a variety of virtual machines (VMs) based on your needs, whether it's a small instance for development or a larger one for production. You pay only for the computing power you use, and you can scale up or down depending on traffic.  **Step 2: Data Storage**  You use AWS S3 (Simple Storage Service) to store user data, images, and other files. S3 offers a scalable and cost-efficient storage solution where you only pay for the storage you use. If your app grows and you need more storage, you can increase capacity quickly without worrying about physical infrastructure.  **Step 3: Load Balancing and Traffic Management**  Your web application becomes popular, and you experience increased traffic. You use AWS Elastic Load Balancer (ELB) to distribute the incoming traffic across multiple EC2 instances to ensure high availability and reliability.  **Step 4: Networking and Security**  You set up **Virtual Private Cloud (VPC)** to create a secure and isolated network within AWS, ensuring that your data and application remain safe. You also configure **firewalls** and **security groups** to control which traffic is allowed to access your servers.  **Step 5: Scaling Based on Demand**  During busy periods (e.g., during product launches or sales), your web traffic spikes. Thanks to IaaS, you can quickly scale up by adding more EC2 instances, ensuring that your application continues to perform well without any downtime. When the traffic decreases, you can scale down to save costs. |
| PaaS (Platform as a service) | **PaaS (Platform as a Service)** is a cloud computing model that provides a platform allowing developers to build, deploy, and manage applications without having to manage the underlying infrastructure. In simpler terms, PaaS provides the hardware and software tools necessary for application development, such as operating systems, databases, middleware, and development tools—everything needed for building applications, minus the need to worry about managing the infrastructure itself (like servers or storage). | Example: - If we are part of a small **e-commerce startup** that wants to quickly set up an online store to sell products. Your startup needs a platform to handle online orders, payments, and customer profiles, but you don’t want to spend time managing servers, databases, or handling infrastructure. Instead, you want to focus on enhancing the user experience and growing your business.  **How Shopify (PaaS) Fits into This**:  **1.Quick Setup and Development**:   * Shopify provides pre-built templates for store design, so you don’t need to worry about creating a website from scratch. You can customize the templates to suit your branding and user experience goals. * Shopify's **drag-and-drop interface** allows you to quickly build a user-friendly e-commerce website with integrated shopping cart functionality.   2 **Payment Processing and Online Orders**:   * Shopify has built-in payment gateways like **Shopify Payments**, **PayPal**, and **Stripe** to process transactions securely. You don’t need to worry about integrating external payment systems or handling the complexities of online payments. * It automatically handles the order processing, including order confirmation, invoicing, and inventory updates.   3. **Database and Infrastructure Management**:   * Shopify hosts the entire platform for you. You don't need to worry about managing databases or servers. It automatically manages the hosting infrastructure, ensuring that your website is scalable and can handle high traffic, especially during sales or promotions. * The platform is built for scalability, so as your business grows and traffic increases, Shopify will handle the infrastructure changes, such as adding more resources and ensuring your site remains fast and responsive.   4. **Customer Profiles and Data Management**:   * Shopify automatically collects and stores customer data, such as purchase history, shipping addresses, and payment information, which you can access through the Shopify Admin interface. * You can set up personalized marketing campaigns, track customer behaviours, and offer tailored discounts without worrying about managing complex databases.   5. **Integrated Marketing and SEO Tools**:   * Shopify provides built-in tools for marketing your e-commerce site, including **SEO optimization**, **email marketing**, and **social media integration**. * It allows you to integrate with third-party marketing tools, and you can track sales conversions directly within the platform.   6. **Analytics and Reporting**:   * Shopify provides built-in analytics and reporting features, allowing you to track sales, orders, inventory levels, and customer behavior. You can make data-driven decisions without needing to set up complex reporting tools.   7. **Security and Compliance**:   * Shopify handles the security and compliance aspects of running an e-commerce store, including PCI DSS compliance for payment data. This means you don’t need to worry about security patches or managing encryption—Shopify ensures your customers' data is secure.   8. **Mobile App Support**:   * Shopify offers a mobile app, enabling you to manage your store, view sales, track inventory, and communicate with customers on the go. |
| SaaS (Software as a service) | **SaaS (Software as a Service)** is a cloud computing model that delivers software applications over the internet, on a subscription basis. Instead of purchasing and installing software on individual computers or servers, users can access and use the software via a web browser. The software is hosted, maintained, and managed by a third-party service provider, freeing users from the responsibility of managing infrastructure, updates, and security.  In SaaS, everything—from the application itself to the underlying infrastructure—is managed by the provider, and users only need a device and internet connection to access the software. | **Real-World Example of Using SaaS:**  Let’s imagine you're a **freelance graphic designer** managing multiple clients and projects. You need tools for project management, communication, file storage, and client invoicing. Instead of purchasing separate software for each function and managing the infrastructure yourself, you decide to use **SaaS (Software as a Service)** applications to streamline your work.  **Step 1: Project Management with Trello**  You use **Trello**, a SaaS project management tool, to organize your tasks and keep track of deadlines for your clients. With Trello, you create boards for each project, add tasks like "Design Logo," "Create Social Media Graphics," and "Finalize Brochure," and assign due dates.   * **How it works**: You don’t need to install any software on your computer. Simply log in to **Trello** through your web browser, and all your project boards are accessible from any device with an internet connection. You can easily track your progress, collaborate with clients, and keep everything organized.   **Step 2: Communication with Slack**  For team communication and collaboration with your clients, you use **Slack**, a SaaS messaging platform. In Slack, you create different channels for each client or project, where you can easily share updates, files, and feedback.   * **How it works**: You and your clients can communicate instantly, send direct messages, share files, and have real-time discussions without the need for email or meeting interruptions. Slack allows you to stay in touch with clients and collaborators seamlessly, whether you’re at home, in a cafe, or on the go.   **Step 3: File Storage with Google Drive**  To store and share your design files, you use **Google Drive**, a cloud-based file storage service. With Google Drive, you can upload your large design files, such as PSDs or vector illustrations, and organize them into folders for each client or project.   * **How it works**: All your files are securely stored in the cloud and are accessible from anywhere with an internet connection. You can share files with clients and collaborators via links and control the permissions (view or edit) without worrying about sending large email attachments.   **Step 4: Invoicing with FreshBooks**  For client invoicing and accounting, you use **FreshBooks**, a cloud-based SaaS accounting tool. FreshBooks helps you create professional invoices, track time worked on client projects, and handle payments easily.   * **How it works**: You log in to your **FreshBooks** account to generate an invoice for a completed project, and it’s automatically sent to the client via email. The platform also tracks your payments, generates reports for tax season, and integrates with your bank accounts. You can manage everything from one platform without needing any accounting software installed.   **Step 5: Cloud Backup and Security with Dropbox**  To ensure your work is backed up and safe, you use **Dropbox** as an additional file storage service for important project files and backups. Dropbox automatically syncs your files between devices and provides additional cloud storage space.   * **How it works**: Your design files are saved and synced automatically across your devices. In case your computer fails or if you need to access your files on a different device, you can securely access them from anywhere. |

# Day 1: Task 3

Please research the below terms and explain what they are, when they would be appropriate and a real-world example of where it could be implemented (i.e. what type of organisation).

|  |  |
| --- | --- |
| Public Cloud | A **Public Cloud** is a type of cloud computing environment where computing resources such as servers, storage, and applications are provided and managed by third-party cloud service providers over the internet. These resources are made available to the public, and multiple organizations (or tenants) share the same infrastructure.  In a public cloud, the cloud provider owns and operates the hardware and software infrastructure, while users can access and use services on a pay-as-you-go or subscription basis. The infrastructure is typically shared among multiple customers, meaning that users share resources like computing power and storage with other organizations. However, each user's data and applications remain isolated and secure. |
| Private Cloud | A **Private Cloud** is a cloud computing environment that is exclusively used by one organization or entity. Unlike a **Public Cloud**, where resources (servers, storage, etc.) are shared with other users, a private cloud provides dedicated infrastructure that is either hosted internally (on-premises) or externally (by a third-party service provider) but used solely by one organization.  Private clouds offer many of the same benefits as public clouds—such as scalability, flexibility, and on-demand resources—but they provide more control, security, and customization because the infrastructure is not shared with others. |
| Hybrid Cloud | A **Hybrid Cloud** is a cloud computing environment that combines elements of both **public** and **private** clouds, allowing data and applications to be shared between them. The hybrid cloud architecture enables businesses to take advantage of the scalability and cost-effectiveness of public clouds, while maintaining the security, control, and customization of private clouds for sensitive workloads.  In a hybrid cloud setup, an organization can run critical applications and store sensitive data on a private cloud (or on-premises infrastructure) while leveraging public cloud resources for less sensitive operations, like running applications that require scalability or burst capacity. |
| Community Cloud | A **Community Cloud** is a type of cloud computing environment that is shared and used by multiple organizations with similar interests, requirements, or goals. Unlike a **Public Cloud**, where services and infrastructure are available to the general public, a community cloud is designed for a specific community of users (such as organizations within the same industry, region, or with similar regulatory requirements). These organizations share the infrastructure, but the cloud is tailored to meet their specific needs.  Community clouds are typically managed and operated by a third-party cloud service provider or by the community itself. The key is that the cloud infrastructure is dedicated to a specific group rather than being open to the public. |

# Day 2: Task 1

Describe, with examples, the **three** major areas that the Computer Misuse Act deals with.

|  |  |  |
| --- | --- | --- |
| Area | Description | Example |
| Unauthorized Access to Computer Material | This section criminalizes gaining access to a computer system or network without permission. It’s commonly referred to as **hacking**. | * A person who uses software tools to guess or bypass login credentials and gains unauthorized access to a company's database or an individual's social media account is committing this offence. Even if no data is stolen or altered, simply accessing the system without authorization is illegal.   **2. Unauthorized Access with Intent to C** |
| Unauthorized Access with Intent to Commit Further Offences | This offence extends beyond just accessing a computer system. It covers situations where unauthorized access is gained with the intent to commit additional illegal actions, such as fraud, theft, or data manipulation. | A hacker gains access to a company’s financial records and intends to steal sensitive information for identity theft or financial fraud. Even if the hacker doesn't carry out the theft immediately, the intent to commit further criminal activity upon accessing the system makes this an offence. |
| Unauthorized Modification of Computer Material | This section targets actions that alter or destroy data on a computer system without permission. This includes modifying, deleting, or damaging data, or disrupting the functionality of the computer or network. | A person installs malware or a virus on a company's servers, causing data corruption, loss, or rendering the systems unusable. This type of behaviour is illegal under the Computer Misuse Act because it causes harm to the integrity and availability of computer systems and data. |

The computer misuse act 1990 is an act where an individual can be criminalised because of computer related offense. Describe three extra powers that the Police and Justice Act 2006 (Computer Misuse) has added.

|  |
| --- |
| Description |
| The Police and Justice Act 2006 introduced several significant changes to the Computer Misuse Act 1990, particularly to address new types of cybercrime and improve the effectiveness of law enforcement in dealing with computer-related offenses. Here are three extra powers added by the Act: |
| 1. Unauthorized Modification of Computer Material (Section 36)   * Power Added: The Act made it easier for law enforcement to prosecute individuals who intentionally or recklessly cause damage to computer material by introducing unauthorized modification as a criminal offense. * Explanation: This provision specifically targets those who introduce viruses or malware, destroy or alter data, or tamper with computer systems, even if no direct damage to hardware occurs. It allows police to act in cases where there is a reckless disregard for the security or integrity of computer systems.   2. Powers of Search and Seizure (Section 19)   * Power Added: The Police and Justice Act 2006 introduced more specific powers to allow law enforcement to search premises and seize computer equipment that is suspected to have been used in committing offenses under the Computer Misuse Act. * Explanation: Law enforcement officers were granted the ability to seize computers, storage devices, and relevant data to investigate any suspected offenses more effectively. This was critical in cases involving cybercrime, where the evidence is often stored on digital devices, making it easier to gather evidence in cases like hacking or unauthorized access.   3. Powers of Search and Seizure (Section 19)   * Power Added: The Police and Justice Act 2006 introduced more specific powers to allow law enforcement to search premises and seize computer equipment that is suspected to have been used in committing offenses under the Computer Misuse Act. * Explanation: Law enforcement officers were granted the ability to seize computers, storage devices, and relevant data to investigate any suspected offenses more effectively. This was critical in cases involving cybercrime, where the evidence is often stored on digital devices, making it easier to gather evidence in cases like hacking or unauthorized access. |
|  |

Look at the below website to answer the questions:

<https://www.gov.uk/personal-data-my-employer-can-keep-about-me>

|  |
| --- |
| Write down three items of data which a company can store about an employee. |
| * Name * Address * Date of birth |
|  |
|  |

|  |
| --- |
| Give three more examples of data that an employer can only store if they first get the employee’s permission. |
| * Race and ethnicity * Religion * health and Medical Condition |
|  |
|  |

Conduct further research to answer the below questions.

|  |  |
| --- | --- |
| Question | Answer |
| Provide one example of: Copyright infringement | Suppose a **graphic designer** creates a unique logo for a company and holds the copyright to that logo. However, a different company, without permission, copies the logo and uses it for their own branding on their website and promotional materials.  This would be an example of copyright infringement because the second company is using the designer's logo without authorization, violating the designer's exclusive rights to reproduce and distribute their work. The designer could take legal action to stop the use and seek damages. |
| Provide one example of: Plagiarism | A student is assigned an essay on climate change. Instead of researching and writing the essay themselves, the student copies large portions of text from a website without giving credit to the original author or citing the source. The student submits the essay as their own work.  This is an example of **plagiarism**, as the student is presenting someone else's work, ideas, or writing as their own without proper attribution or citation. This is a violation of academic integrity. |
| What are two consequences of copyright infringement and software piracy? | 1. **Legal Consequences:**   * **Copyright infringement** and **software piracy** can result in legal action being taken against the offender. This could involve civil lawsuits where the copyright holder seeks monetary compensation for damages, or even criminal charges in severe cases. The penalties can include fines, orders to pay damages, and in some cases, imprisonment for those found guilty of large-scale piracy or repeated violations.   2. **Reputational Damage:**   * Being caught for copyright infringement or software piracy can severely damage an individual’s or business’s reputation. It can lead to loss of trust among customers, partners, and stakeholders. In business, this might also result in lost sales, contracts, and future opportunities. |
| Give three possible consequences for individuals when using pirated software | 1. **Legal Consequences:**   * **Risk of Legal Action**: Using pirated software is illegal, and individuals could face legal action from the software developers or copyright holders. This could result in hefty fines or even criminal charges, depending on the scale of the infringement. * **Example**: An individual caught using pirated software could face a lawsuit or be penalized with a fine for copyright infringement.   2. **Security Risks:**   * **Malware and Viruses**: Pirated software often comes from unreliable sources and can be bundled with malware, viruses, or ransomware. This can compromise the security of personal data, cause system malfunctions, or lead to identity theft. * **Example**: Using pirated software might expose an individual's computer to harmful software, leading to data breaches or loss of sensitive information.   3. **Lack of Support and Updates:**   * **No Official Support**: Pirated software typically does not have access to official updates, bug fixes, or technical support. This means users miss out on security patches, feature enhancements, and may face difficulties with software compatibility or functionality. * **Example**: An individual using pirated software might not be able to update it when a new security vulnerability is discovered, making their system more prone to cyberattacks. |

Listed below are some laws which we have covered today:

1. Computer Misuse Act 1990

2. Police and Justice Act 2006 (Computer Misuse)

3. Copyright, Designs and Patents Act 1988

4. Copyright (Computer Programs) Regulations 1992

5. The Health and Safety (Display Screen Equipment) Regulations 1992

6. Data Protection Act 2018

7. Consumer Rights Act 2015

* Insert a number in the first column of each row to match each of the statements with one of the above Acts.
* One of statements is incorrect and not illegal. For this statement, write ‘Not illegal’.

|  |  |
| --- | --- |
| **Act number** | **Clause** |
| 1988 | With some exceptions, it is illegal to use unlicensed software |
| 1979 | Any product, digital or otherwise, must be fit for the purpose it is supplied for |
| 1990 | Unauthorised modification of computer material is illegal |
| 1990, specifically under section 3A | It is illegal to create or use a hacking tool for penetration testing |
| 2018(GDPR) | Personal data may only be used for specified, explicit purposes |
| DPA2018 | Personal data may only be used for specified, explicit purposes |
| Computer Misuse Act 1990, Section 3A | It is illegal to distribute hacking tools for criminal purposes |
| Copyright, Designs and Patents Act 1988. | It is illegal to distribute an illicit recording |
| Data Protection Act 2018 | Personal data may not be kept longer than necessary |
| Computer Misuse Act 1990, Section **1** | Gaining unauthorised access to a computer system is illegal |
| Health and Safety Regulation 1992 | Employers must ensure that employees take regular and adequate breaks from looking at their screens |
| Computer Misuse Act 1990, Section 3 | It is illegal to prevent or hinder access (e.g. by a denial-of-service attack) to any program or data held in any computer |
| Data Protection Act 2018 (GDPR) | Personal data must be accurate and where necessary kept up to date |

# Day 3: Task 1

Please complete the below lab (3) *‘Explore relational data in Azure’* and paste evidence of the completed lab in the box provided.



|  |  |
| --- | --- |
| Completed lab |  |

# Day 3: Task 2

Please complete the below lab (4) *‘Explore non-relational data in Azure’* and paste evidence of the completed lab in the box provided.



|  |  |
| --- | --- |
| Completed lab |  |

# Day 4: Task 1

In your teams, complete the Azure DP-900 practice exam and paste your result below – this is open book and please research and discuss your answers as a team.



|  |  |
| --- | --- |
| Result |  |

# Day 4: Task 2

#### **1. Scenario Background**

"Paws & Whiskers" is a growing pet shop that aims to improve its business by analysing sales, customer information, and inventory data. Currently, the data is collected manually or stored in spreadsheets. Management is interested in transitioning to Microsoft Azure to streamline data storage, analysis, and reporting, enabling them to make data-driven decisions.

#### **2. Data Laws and Regulations**

Identify and explain the data laws and regulations relevant to handling customer data within the proposal. Ensure you cover the following points:

* **GDPR Compliance**: Highlight the importance of adhering to the General Data Protection Regulation (GDPR), particularly as it relates to storing and processing customer information.
* **Data Protection Act (DPA) 2018**: Outline how the DPA 2018 may affect the way "Paws & Whiskers" collects and stores data, ensuring compliance with UK laws on data privacy.
* **Other Industry Standards**: Research any additional data protection standards or regulations that may apply to pet shop data, particularly if they involve sensitive or payment information.

#### **3. Azure Service Recommendations**

Recommend Microsoft Azure services that would suit the company’s data analysis needs and explain why these services are suitable. Your recommendations should include:

* **Data Storage**: Identify suitable storage options, such as **Azure Blob Storage** or **Azure SQL Database**, and discuss the benefits of each for storing large datasets, including inventory, sales transactions, and customer details.
* **Data Analysis Tools**: Recommend tools such as **Azure Machine Learning** for customer behaviour analysis or **Azure Synapse Analytics** for analysing sales trends.
* **Data Integration and Automation**: Explain how services like **Azure Data Factory** could automate data collection and integration processes, improving efficiency.

#### **4. Data Types and Data Modelling**

Define the types of data "Paws & Whiskers" will need to work with and describe your approach to data modelling:

* **Data Categories**: Identify key data types, such as customer demographics, transaction history, pet inventory, and product categories.
* **Data Modelling Approach**: Outline how you would structure this data using a relational model or a data warehouse approach, considering factors like tables, entities, relationships, and primary keys.

#### **5. Data Storage Formats and Structures in Azure**

Discuss how you would store data within Azure and the formats you would recommend:

* **Data Formats**: Specify recommended formats (e.g., CSV for raw data imports, JSON for structured data, Parquet for analytics) and explain why these formats are suitable for specific data types.
* **Data Security and Encryption**: Include recommendations for securing data using Azure’s built-in encryption features and access controls to ensure compliance with data privacy regulations.

#### **6. Additional Considerations**

Provide any other considerations that might enhance data handling and efficiency in Azure, such as:

* **Backup and Disaster Recovery**: Outline a backup plan using **Azure Backup** or **Azure Site Recovery** to safeguard against data loss.
* **Data Visualisation**: Discuss potential use of **Power BI** within Azure for creating dashboards that provide management with real-time insights into sales and customer trends.
* **Future Scalability**: Comment on how Azure services can scale as the business grows, accommodating larger datasets and more complex analyses.

### **Submission Guidelines:**

1. **Structure**: Ensure your report is well-organised, with sections for each task (e.g., Data Laws, Azure Services, Data Types, etc.).
2. **Formatting**: Include headings, bullet points where appropriate, and any visuals or diagrams that support your explanations.
3. **References**: Cite any resources or regulations referenced in the report.
4. **Length**: Aim for 1500-2000 words.

|  |
| --- |
|  |

|  |
| --- |
| **Course Notes** |

It is recommended to take notes from the course, use the space below to do so, or use the revision guide shared with the class:

|  |
| --- |
| **Additional Information** |

We have included a range of additional links to further resources and information that you may find useful, these can be found within your revision guide.

**END OF WORKBOOK**

**Please check through your work thoroughly before submitting and update the table of contents if required.**

**Please send your completed work booklet to your trainer.**