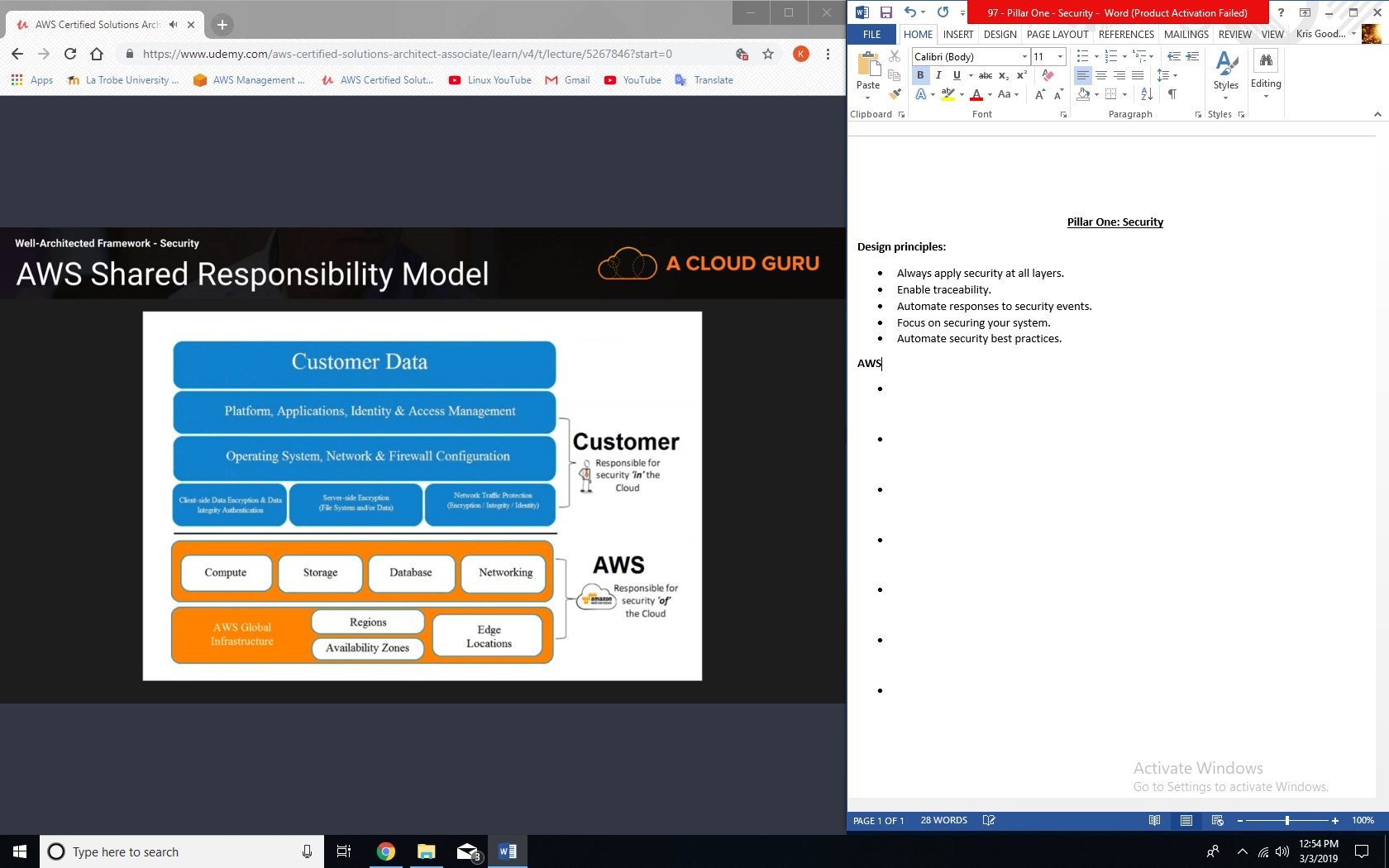
**Pillar One: Security**

**Design principles:**

* Always apply security at all layers.
* Enable traceability.
* Automate responses to security events.
* Focus on securing your system.
* Automate security best practices.

**AWS Shared Responsibility Model:**

**Definition:**

* Security in the cloud consists of 4 areas
  + Data protection:
    - Before you begin to architect security practices across your environment, basic data classification should be in place. You should organize and classify your data into segments such as publicly available, available to only members of your organization, available to only certain members of your organization, available only to the board, etc. You should also implement a least privilege access system so that people are only able to access what they need. However most importantly, you should encrypt everything where possible, whether it be at rest or in transit.
    - In AWS, the following practices help to protect your data;
      * AWS customers maintain full control over their data.
      * AWS makes it easier for you to encrypt your data and manage keys, including regular key rotation, which can be easily automated natively by AWS or maintained by a customer.
      * Detailed logging is available that contains important content, such as file access and changes.
      * AWS has designed storage systems for exceptional resilience. As an example, Amazon Simple Storage Service (S3) is designed for 11 nines of durability. (For example, if you store 10,000 objects with Amazon S3, you can on average expect to incur a loss of a single object once every 10,000,000 years.)
    - Versioning, which can be part of a larger data lifecycle-management process, can protect against accidental overwrites, deletes, and similar harm.
    - AWS never initiates the movement of data between regions. Content placed in a region will remain in that region unless the customer explicitly enables a feature that leverages a service that provides that functionality.
  + Privilege management:
    - Privilege management ensures that only authorized and authenticated users are able to access your resources, and only in a manner that is intended. It can include:
      * Access Control Lists (ACLs)
      * Role Based Access Controls
      * Password Management (such as password rotation policies)
    - Privilege management questions:
      * How are you protecting access to and use of the AWS root account credentials?
      * How are you defining roles and responsibilities of system users to control human access to the AWS Management Console and APIs?
      * How are you limiting automated access (such as from applications, scripts, or third-party tools or services) to AWS resources.
      * How are you managing keys and credentials
  + Infrastructure protection:
    - Outside of cloud, this is how you protect your data center. RFID controls, security, lockable cabinets, CCTV, etc. Within AWS, they handle this, so really infrastructure protection exists at a VPC level.
    - Infrastructure Protection Questions:
      * How are you enforcing network and host-level boundary protection?
      * How are you enforcing AWS service level protection?
      * How are you protecting the integrity of the operating systems on your Amazon EC2 instance?
  + Detective controls:
    - You can use detective controls to detect or identify a security breach.
    - AWS services to achieve this include:
      * AWS CloudTrail.
      * Amazon CloudWatch.
      * AWS Config.
      * Amazon Simple Storage Service (S3).
      * Amazon Glacier.
    - Detective control questions:
      * How are you capturing and analyzing AWS Logs

**AWS Key Services**

* Data protection:
  + You can encrypt your data both in transit and at rest using; ELB, EBS, S3, & RDS.
* Privilege management:
  + IAM, MFA.
* Infrastructure protection:
  + VPC.
* Detective controls:
  + AWS CloudTrail, AWS Config, Amazon CloudWatch.

**Exam Tips – Security Pillar**

* Security in the cloud consists of 4 areas;
  + Data protection
  + Privilege management
  + Infrastructure protection
  + Detective controls

**Exam Tips – Security Pillar – Questions**

* Data protection:
  + How are you encrypting and protecting your data at rest?
  + How are you encrypting and protecting your data in transit? (SSL)
* Privilege management:
  + How are you protecting access to and use of the AWS root account credentials
  + How are you defining roles and responsibilities of system users to control human access to the AWS Management Console and APIs?
  + How are you limiting automated access (such as from applications, scripts, or third-party tools or services) to AWS resource?
  + How are you managing keys and credentials?
* Infrastructure protection:
  + How are you enforcing network and host-level boundary protection?
  + How are you enforcing AWS service level protection?
  + How are you protecting the integrity of the operating systems on your Amazon EC2 instance?
* Detective controls:
  + How are you capturing and analyzing AWS logs?