- ## Phase 1 - Security

Security Design Principles

There are seven design principles for security in the cloud:

- **Implement a strong identity foundation**: Implement the principle of least privilege and enforce separation of duties with the appropriate authorization for each interaction with your AWS resources. Centralize identity management, and aim to eliminate reliance on long-term static credentials.

- **Enable traceability**: Monitor, alert, and audit actions and changes to your environment in real-time. Integrate log and metric collection with systems to investigate and take action automatically.

- **Apply security at all layers**: Apply a defense in depth approach with multiple security controls. Apply to all layers (for example, edge of the network, VPC, load balancing, every instance and compute service, operating system, application, and code).

- **Automate security best practices**: Automated software-based security mechanisms improve your ability to scale more rapidly and cost-effectively securely. Create secure architectures, including implementing controls that are defined and managed as code in version-controlled templates.

- **Protect data in transit and at rest**: Classify your data into sensitivity levels and use mechanisms such as encryption, tokenization, and access control where appropriate.

- **Keep people away from data**: Use mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This reduces the risk of mishandling, modification, and human error when handling sensitive data.

- **Prepare for security events**: Prepare for an incident by having incident management and investigation policy and processes that align with your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

Security Evaluation Questions:

1. How do you securely operate your workloads on AWS?
2. How do you manage identities for people and machines?
3. How do you manage permissions for people and machines?
4. What Services are you using to detect and remediate security events?
    a. Application Hosting?

    b. Storage?
    c. Networking?
    d. Datastores?
    e. Infrastructure?
5. How do you protect your network resources?
6. How do you protect your compute resources?
7. How do you classify your data?
8. How do you protect data at rest?
9. How do you protect data in transit?

Apply these to your design. Update the design. Commit the design to the repository.