1. *Risk Assessment: Identify top three potential threats to AWS landing zone and suggest mitigation strategies for each*

1) **Data Security** - Identify data content being stored/transmitted and sensitivity levels according to company data labeling policy. Apply appropriate hardening templates/AMI's for each computing resource (Container, VM/EC2, etc) and storage level elements (Database, Disk, etc). Ensure appropriate access controls are defined (muti-Account OU strategy) and enforced for direct/raw or downstream access to the data. Where data is in transit, apply necessary encryption protocols (TLS, SSH, etc) to guard against threats of cleartext exposure of contents.

2) **Edge/Network Security** - Configure access to resources in a fashion which eliminates unnecessary exposure to services or interfaces to unintended audiences. Utilize AWS firewall/WAF for perimeter, an appropriately configured Transit Gateway or DirectConnect with ACLs for network peering/interconnectivity and host/resource based firewalls to restrict unnecessary access/blast-radius of compromise.

3) **Inadvertent Misconfiguration** - Utilize IaC (Infrastructure as Code) where feasible and ensure each change/modification is rigorously tested and stored in an enterprise approved code repository. Terraform/ControlTower can be used to deploy CI/CD for automated test/builds. SAST/DAST and other application/code vulnerability scanners should be utilized during build and test phases - while a post implementation verification needs to be performed to ensure changes meet the expected design in production accounts.

2. *Architecture Design: Outline the key components of a secure architecture for the AWS Landing Zone, focusing on a secure foundation for workload and data deployments.*

Data being utilized for this environment needs to be evaluated against the enterprise's data classification policy. If content is considered confidential, then necessary controls to protect the data shall be enforced. Data at rest controls such as file/disk systems using KMS, or data in transit / SSL certificates managed by AWS Certificate Manager - need to be applied.

For securing workloads, ensure access is limited to the compute/application/function/interface accordingly. Access should be provisioned in a least privileged fashion. A multi-account OU strategy, with MFA applied, should grant access to individuals based on job responsibility. The ability to connect to the services should be limited to approved resources (locations, servers, networks, etc) only. Restrict access by network, host, or AWS configured ACLs.

Deploy only approved AMIs or CIS Hardened images for the environment and continuously scan for vulnerabilities using a dedicated tool.

3. Security Requirements: Provide high-level security requirements for the AWS environment as a part of a hybrid, multi-cloud strategy

4. Implementation Plan: Outline the key steps required to deploy a secure Landing Zone focusing on the main phases and critical actions and deliverables

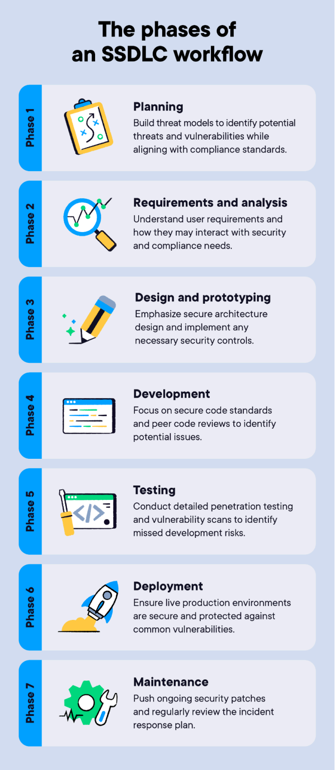
5. Compliance and Governance: Identify the key regulations and industry standards that the AWS landing zone must comply with and outline a governance framework

Utilize an SSDLC approach towards the design, development and build of the Landing Zone.

Review the operational/functional requirements design by business/application stakeholders.

Assess the enterprise's risk appetite for data security and controls. Identify baseline content protection measures and stepped assurances for each increment in risk appetite / data sensitivity labels. Inquire with the enterprise compliance department/staff for which regulatory requirements are necessary for enforcement (FFIEC, FDIC, PCI, NYDFS, etc)

Determine if a control framework has been adopted (NIST, ISO27001, COBIT, PCI, etc), and institute a mapping based on industry guidance from the Center of Internet Security. https://www.cisecurity.org/controls/cis-controls-navigator



The phases of an SSDLC workflow

Phase 1 — Planning: Build threat models to identify potential threats and vulnerabilities while aligning with compliance standards.

Phase 2 — Requirements and analysis: Understand user requirements and how they may interact with security and compliance needs.

Phase 3 — Design and prototyping: Emphasize secure architecture design and implement any necessary security controls.

Phase 4 — Development: Focus on secure code standards and peer code reviews to identify potential issues.

Phase 5 — Testing: Conduct detailed penetration testing and vulnerability scans to identify missed development risks.

Phase 6 — Deployment: Ensure live production environments are secure and protected against common vulnerabilities.

Phase 7 — Maintenance: Push ongoing security patches and regularly review the incident response plan.

Collaborate with technical SME's on the proposed design and ensure base CIS Control categories for the following are being met:

CIS Control	Title	Description
1	Inventory and Control of Enterprise Assets	Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.
2	Inventory and Control of Software Assets	Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
3	Data Protection	Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
4	Secure Configuration of Enterprise Assets and Software	Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
5	Account Management	Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.
6	Access Control Management	Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.
7	Continuous Vulnerability Management	Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.
8	Audit Log Management	Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.
9	Email and Web Browser Protections	Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.
10	Malware Defenses	Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
11	Data Recovery	Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

12	Network Infrastructure Management	Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.
13	Network Monitoring and Defense	Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.
14	Security Awareness and Skills Training	Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.
15	Service Provider Management	Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.
16	Application Software Security	Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.
17	Incident Response Management	Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.
18	Penetration Testing	Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Identify and suggest any necessary corrective negligences or shortcomings in security controls. Incorporate AWS Landing Zone specific best principles: https://docs.aws.amazon.com/whitepapers/latest/nhs-cloud-security-guidance-using-aws/overall-security-governance---aws-landing-zones.html

- Principle 1: Data in transit protection
- Principle 2: Asset protection and resilience
- Principle 3: Separation between users
- Principle 4: Governance framework
- Principle 5: Operational security
- Principle 6: Personnel security
- Principle 7: Secure development
- Principle 8: Supply chain security
- Principle 9: Secure user management
- Principle 10: End user identity and authentication
- Principle 11: External interface protection
- Principle 12: Secure service administration
- Principle 13: Audit information for users
- Principle 14: Secure use of the service

Iterate through the development and testing phases with certifications of security baselines being achieved.

Ensure the proposed deployment has undergone/submitted to the enterprise change management board and received all necessary approvals. Schedule the change to be deployed and verify production environments are operating as intended.

Validate security and operating hygiene through ongoing maintenance of the environment. Incorporate the Landing Zone into the scope of security tools and monitoring of staff. Verify that asset and data inventories are updated, along with appropriate documentation.