AEGIS

CLOUD ARCHITECTURE

Cloud Landing Zone Blueprint

Enterprise-grade multi-cloud architecture foundations for AWS, Azure, and GCP with security and governance built-in

Multi-Cloud

Security First

Compliance Ready

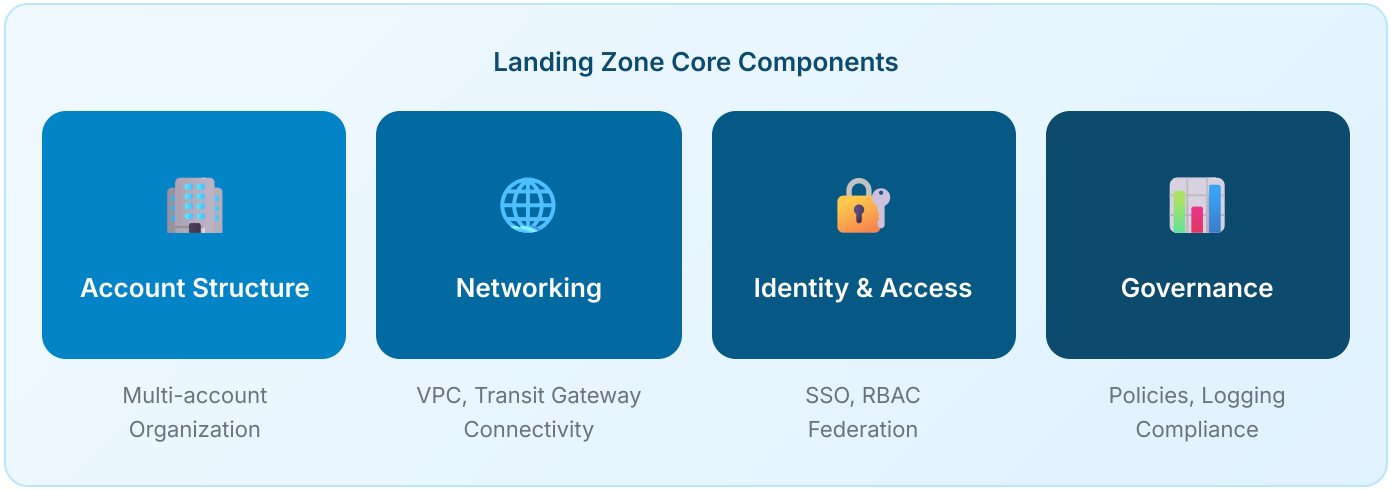
Scalable

Table of Contents

70%	40%	99.99%	100%
Faster Deployment	Cost Reduction	Uptime SLA	Audit Ready

1. What is a Landing Zone?

A landing zone is a pre-configured, secure, multi-account cloud environment based on best practices. It provides the foundation for workload migration and cloud-native development.



Why Landing Zones Matter

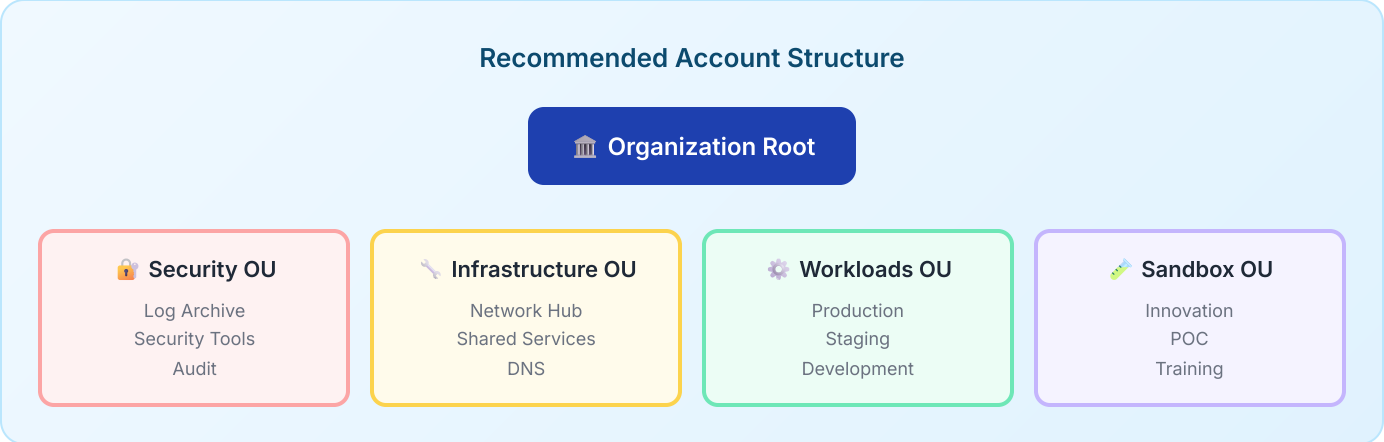
Without Landing Zone	With Landing Zone
❌ Manual, inconsistent setup	✅ Automated, repeatable deployments
❌ Security gaps and misconfigurations	✅ Security best practices enforced
❌ Compliance achieved after-the-fact	✅ Compliance built-in from day one
❌ Difficult to scale and maintain	✅ Designed for growth and change
❌ Cost overruns and waste	✅ Cost visibility and optimization

Key Insight

Organizations with well-designed landing zones deploy workloads 70% faster and experience 80% fewer security incidents compared to ad-hoc cloud environments.

2. Multi-Account Architecture

A multi-account strategy provides blast radius isolation, simplified billing, and clear separation of duties.



Account Purpose Matrix

Account	Purpose	Key Services	Access Level
Management	Organization root, billing	Organizations, Billing, SSO	Admin only
Log Archive	Centralized logging	S3, CloudTrail, Config	Read-only
Security Tools	Security monitoring	GuardDuty, Security Hub	Security team
Network Hub	Centralized networking	Transit Gateway, VPN	Network team
Shared Services	Common tools	CI/CD, Artifacts, DNS	DevOps
Workload Accounts	Application hosting	EC2, EKS, RDS, etc.	App teams

3. Cloud Provider Landing Zones

Each major cloud provider offers native landing zone solutions with similar concepts but different implementations.

AWS

Control Tower + Landing Zone Accelerator

- ✓ Account Factory automation
- ✓ Service Control Policies
- ✓ AWS SSO integration
- ✓ Guardrails (preventive/detective)
- ✓ Customization via CDK

Azure

Cloud Adoption Framework Landing Zone

- ✓ Management group hierarchy
- ✓ Azure Policy & Blueprints
- ✓ Azure AD integration
- ✓ Enterprise-scale architecture
- ✓ Terraform/Bicep modules

GCP

Cloud Foundation Fabric

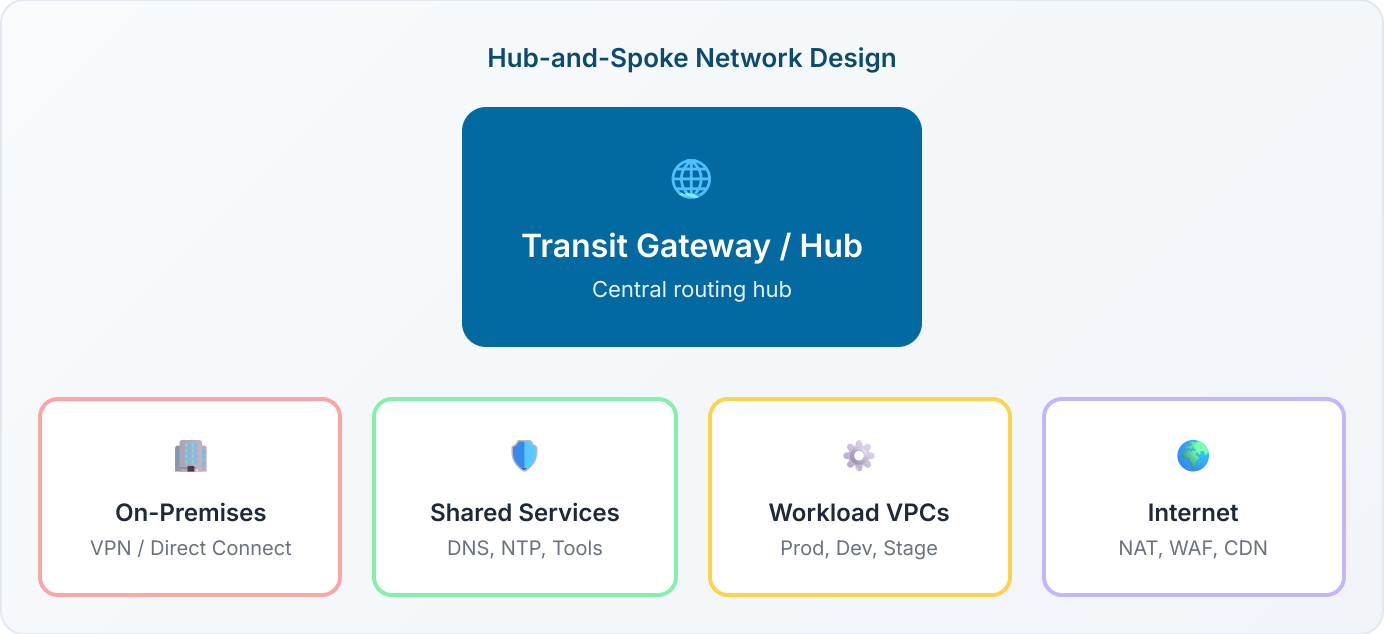
- ✓ Folder hierarchy
- ✓ Organization policies
- ✓ Cloud Identity federation
- ✓ VPC Service Controls
- ✓ Terraform modules

Multi-Cloud Considerations

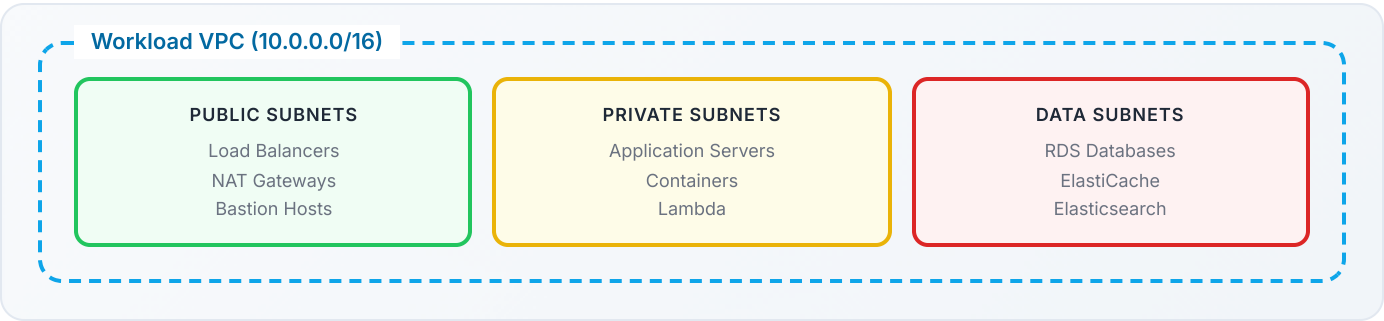
Factor	AWS	Azure	GCP
Best For	Broadest services	Microsoft ecosystem	Data/ML workloads
Maturity	Most mature	Enterprise-focused	Developer-focused
Pricing Model	Per-second billing	Per-minute billing	Per-second billing
Compliance	100+ certifications	90+ certifications	80+ certifications
IaC Support	CDK, CloudFormation, TF	Bicep, ARM, Terraform	Deployment Manager, TF

4. Network Architecture

Hub-and-spoke topology provides centralized control, simplified security, and efficient routing across your cloud environment.



VPC Subnet Design



Key Networking Decisions

CIDR Planning

Use non-overlapping ranges. Reserve space for growth. Document allocations centrally.

DNS Strategy

Centralized DNS in shared services. Private hosted zones for internal resolution.

5. Security Foundations

Defense in depth with multiple security layers ensures protection even if one control fails.

Perimeter Security

WAF, DDoS protection, CDN edge security, API gateway rate limiting

Identity & Access

SSO, MFA enforcement, RBAC, service accounts, least privilege

Network Security

Security groups, NACLs, VPC flow logs, network segmentation

Workload Protection

Endpoint protection, container scanning, runtime security, patching

Data Security

Encryption at rest/transit, key management, DLP, classification

Security Services by Cloud

Capability	AWS	Azure	GCP
SIEM	Security Hub	Microsoft Sentinel	Chronicle
Threat Detection	GuardDuty	Defender for Cloud	Security Command
Secrets	Secrets Manager	Key Vault	Secret Manager
Identity	IAM + SSO	Azure AD	Cloud Identity
WAF	AWS WAF	Azure WAF	Cloud Armor

6. Compliance Frameworks

Landing zones can be pre-configured to meet various compliance requirements, accelerating certification timelines.

FedRAMP

Federal cloud security standard. Required for US government contracts.

StateRAMP

State & local government security. Based on FedRAMP controls.

SOC 2

Trust service criteria for service organizations. Type I & Type II.

HIPAA

Healthcare data protection. PHI security and privacy rules.

PCI DSS

Payment card security. Required for card data handling.

ISO 27001

International security standard. Information security management.

Compliance Automation

Control Area	Automated Solution	Evidence Collection
Access Control	SCPs, IAM policies, RBAC	CloudTrail, Access Analyzer
Encryption	KMS policies, TLS enforcement	Config rules, Security Hub
Logging	Centralized log aggregation	CloudWatch, S3 lifecycle
Network Security	Security groups, NACLs, WAF	VPC flow logs, WAF logs
Vulnerability Mgmt	Inspector, container scanning	Findings dashboards

Compliance Accelerator

Our landing zones include 200+ pre-configured controls mapped to common frameworks, reducing compliance effort by up to 60%.

7. Implementation Checklist

Use this checklist to ensure your landing zone covers all critical areas before deploying workloads.

🏢 Organization Structure

- ☐ Organization created with consolidated billing
- ☐ OU structure defined and documented
- ☐ Service Control Policies configured
- ☐ Account factory/vending machine ready
- ☐ Tagging strategy implemented

🔐 Identity & Access

- ☐ SSO configured with identity provider
- ☐ MFA enforced for all users
- ☐ Permission sets/roles defined
- ☐ Break-glass procedures documented
- ☐ Service accounts governed

🌐 Networking

- ☐ CIDR ranges allocated and documented
- ☐ Transit Gateway/hub VPC deployed
- ☐ DNS strategy implemented
- ☐ VPN/Direct Connect configured
- ☐ Network segmentation verified

📊 Logging & Monitoring

- ☐ CloudTrail enabled organization-wide
- ☐ Log archive account configured
- ☐ Config rules deployed
- ☐ Security alerts configured
- ☐ Cost alerts set up

🛡️ Security

- ☐ GuardDuty/Defender enabled
- ☐ Security Hub aggregating findings
- ☐ KMS keys created and policies set
- ☐ Encryption defaults enforced
- ☐ Vulnerability scanning enabled

⚙️ Operations

- ☐ IaC repository established
- ☐ CI/CD pipelines configured
- ☐ Backup policies defined
- ☐ Disaster recovery tested
- ☐ Runbooks documented

8. Cost Optimization

A well-designed landing zone includes cost visibility and optimization from day one.

Visibility

Cost allocation tags, budgets, anomaly detection, chargeback reporting

Optimization

Right-sizing, Savings Plans, Reserved Instances, spot instances

Automation

Auto-scaling, scheduled shutdowns, lifecycle policies

Cost Optimization Checklist

Strategy	Typical Savings	Effort
Right-sizing (compute)	20-40%	Low
Reserved Instances (1yr)	30-40%	Low
Savings Plans	20-30%	Low
Spot Instances	60-90%	Medium
Storage tiering	30-50%	Low
Idle resource cleanup	10-25%	Low

40%
Avg. Cost Reduction

$2M+
Typical Annual Savings

3mo
Payback Period

100%
Cost Visibility

AEGIS

Ready to Build Your Landing Zone?

Our cloud architects can help you design and implement an enterprise-grade landing zone tailored to your requirements.

Contact Us

info@aegisit.ai

(404) 490-0234

aegisit.ai