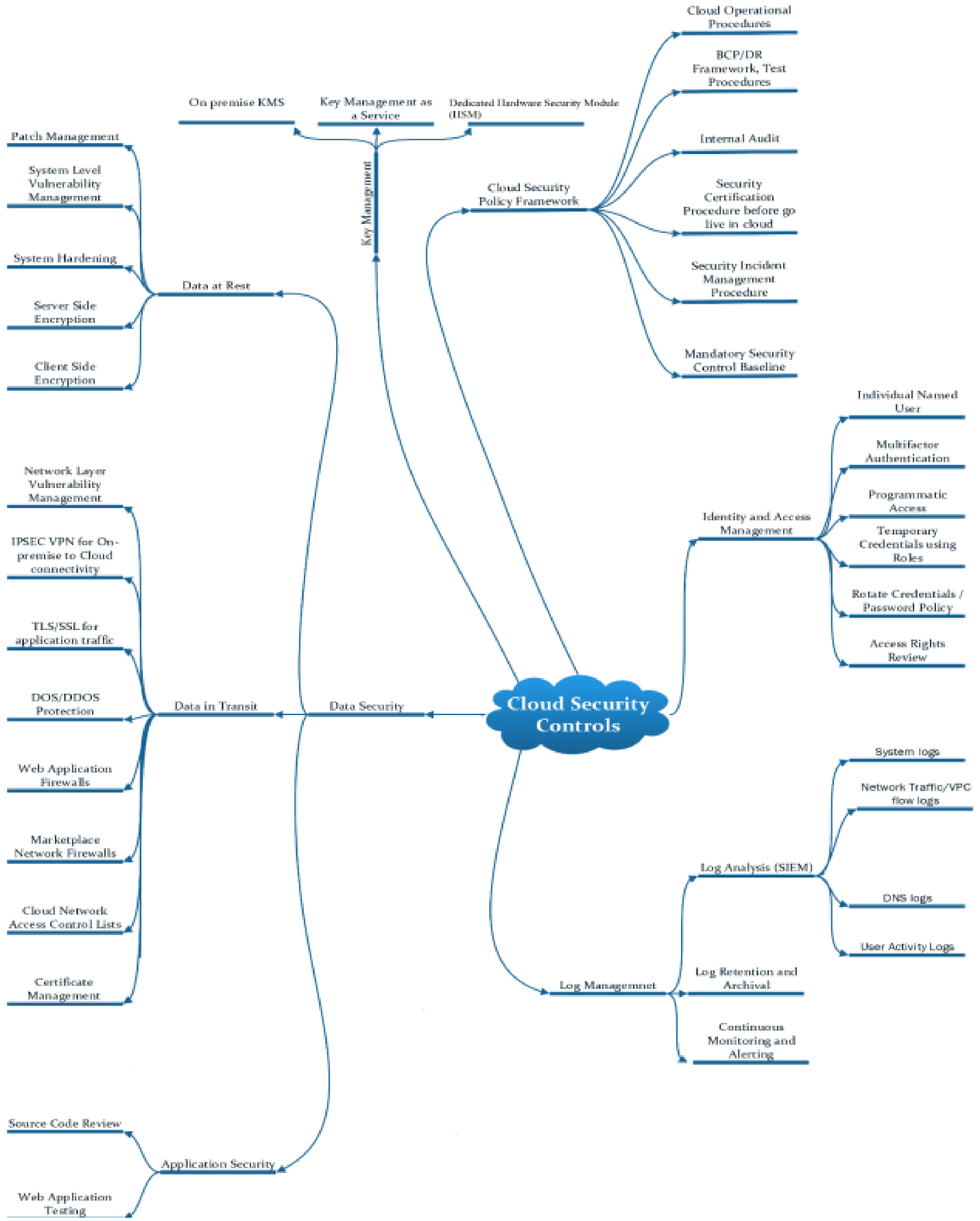
Indicative Mindmap for Cloud Security pointing at Cloud Adoption Framework for SEBI Guidelines – Appendix B


Cloud Security Controls
Key Management
On premise KMS
Key Management as a Service
Dedicated Hardware Security Module (HSM)
Cloud Security Policy Framework
Cloud Operational Procedures
BCP/DR Framework, Test Procedures
Internal Audit
Security Certification Procedure before go live in cloud
Security Incident Management Procedure
Mandatory Security Control Baseline
Identity and Access Management
Individual Named User
Multifactor Authentication
Programmatic Access
Temporary Credentials using Roles
Rotate Credentials / Password Policy
Access Rights Review
Log Managemnet
Log Analysis (SIEM)
System logs
Network Traffic/VPC flow logs
DNS logs
User Activity Logs
Log Retention and Archival
Continuous Monitoring and Alerting
Data Security
Data at Rest
Patch Management
System Level Vulnerability Management
System Hardening
Server Side Encryption
Client Side Encryption
Data in Transit
Network Layer Vulnerability Management
IPSEC VPN for On-premise to Cloud connectivity
TLS/SSL for application traffic
DOS/DDOS Protection
Web Application Firewalls
Marketplace Network Firewalls
Cloud Network Access Control Lists
Certificate Management
Application Security
Source Code Review
Web Application Testing

SEBI MINDMAP FOR CLOUD ADOPTION FRAMEWORK

Cloud Security Controls as per SEBI Guidelines for CAF referring to above mentioned Mindmap

Cloud Security Controls – High Level Details

1. Data Security – The Security Tenet points at Data & Application Security
   a. Data in Transit
   b. Data at Rest
   c. Application Security

2. Key Management - Key Management System at the secrets viz TLS certificates, Secret keys, passphrase in the Vault
3. Identity & Access Management – The Controls pointing at IAAA
4. Log Management – Log Management on the listed Controls
   a. Log analysis (SIEM)
   b. Log Retention & Archival
   c. Continuous Monitoring & Alerting

5. Cloud Security Policy Framework – The overall Governance, Compliance, Hardening, Audit certifications per SEBI directives

S.No	Security Tenet	Category	Sub-Category
1	Data Security	Data in Transit	Network Layer Vulnerability Management
			IPsec VPN for On-Prem to Cloud Connectivity
			TLS/SSL for Application Traffic
			DDoS Protection
			Web Application Firewalls
			Market place Network Firewalls
			Cloud Network Access Control List
			Certificate Management
		Data at Rest	Patch Management
			System Level Vulnerability Management
			System Hardening
			Server Side Encryption
			Client Side Encryption
		Application Security	Source Code Review
			Web Application Testing
2	Key Management	On-Premise KMS	
		Key Management as a Service	
		Dedicated hardware Security Module	
3	Identity & Access Management	Individual Named User	
		Multifactor Authentication	

		Programmatic Access	
		Temporary Credentials using Roles (JIT - Just in Time)	
		Rotate Credentials/Password Policy	
		Access Rights Reviews	
4	Log Management	Log Analysis (SIEM)	System Logs
			Network Traffic/VPC Flow logs
			DNS Logs
			User activity logs
		Log Retention & Archival	
		Continuous Monitoring & Alerting	
5	Cloud Security Policy Framework	Cloud Operational Procedures	
		BCP/DR Framework, Test Procedures	
		Internal Audit	
		Security Certification procedure before go live in Cloud	
		Mandatory Security Control Baseline	

SEBI MINDMAP FOR CLOUD ADOPTION FRAMEWORK

Detailed Work Break Down Structure of the SEBI Cloud Security Controls

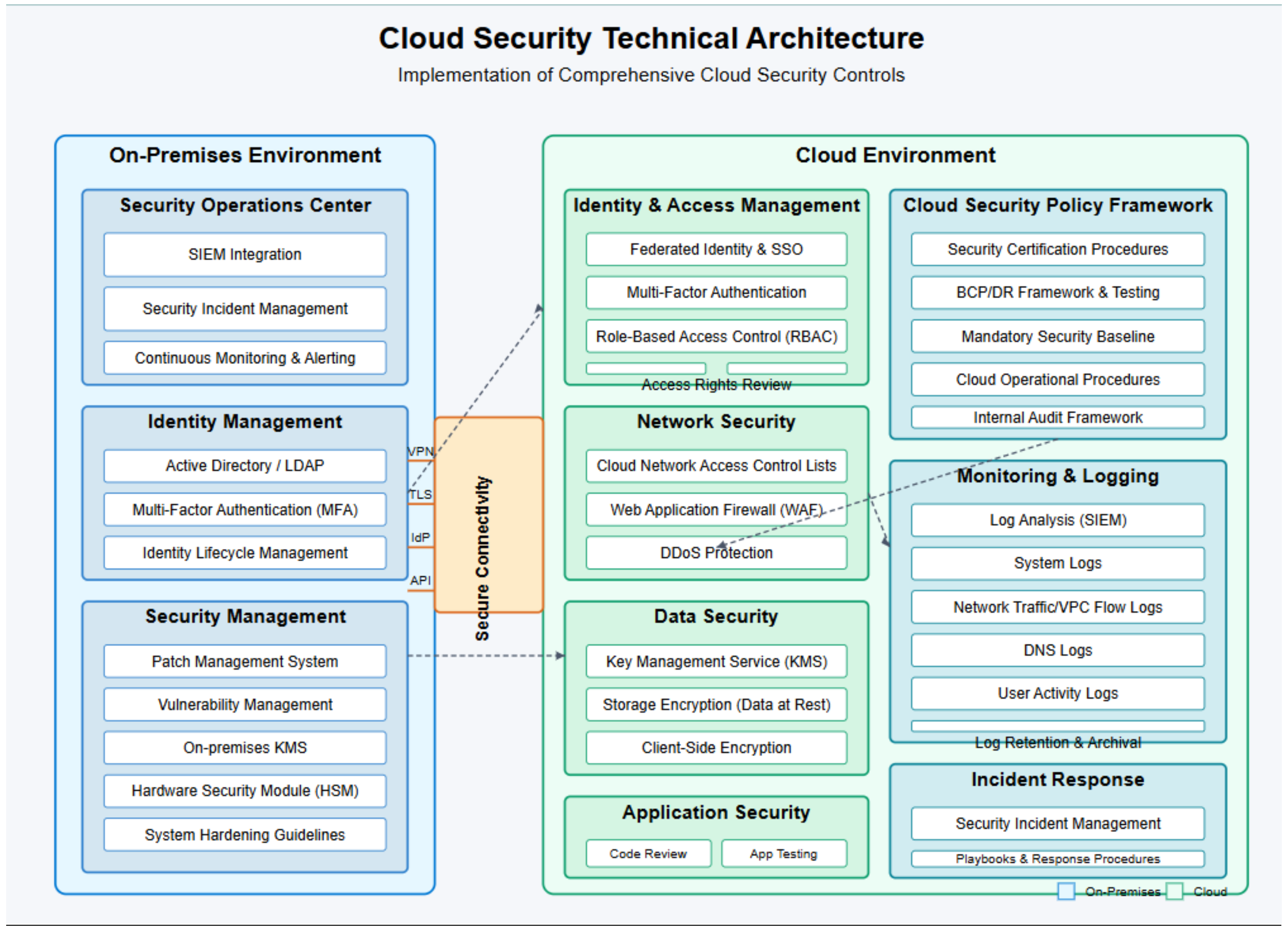
S.No	Security Tenet	Category	Sub-Category	Significance of the Security Tenet	Missing Articulation
1	Data Security	Data in Transit	Network Layer Vulnerability Management	Network Security Penetration for Vulnerabilities at the Device level viz - IDS, IPS, DDoS, Anti-APT, LLB, Switching Stack - L2, L3	Ideally Perimeter Firewalls based Penetration invoked first pointing at Defense in
			IPsec VPN for On-Prem to Cloud Connectivity	a point to point link connectivity via Gateway Device	a. The connectivity could also Express Route fror Could also be Private link with point to point con Cloud application/services b. One can also leverage Zero Trust based conne Principles - Trust but verify, Assume breach alre Tenet, Securing Policy enforcement point, Polic (PeP, PdP)
			TLS/SSL for Application Traffic	TLS or SSL based session for Application that be internal or external	The session could be at the WAN level via Perimte applications, Could also be sustaining at the LA Security
			DDoS Protection	Denial of Service attacks disrupting Availability as per CIA Triad - This denial could be internal or external	
			Web Application Firewalls	WAF is a Technical Control that can be used both externally on WAN as well as on LAN	
			Market place Network Firewalls	Market place Firewalls could be external on WAN at the edge, can also be used Internally on LAN acting as Inner shield - when two of these sets used in Fault Tolerance can compliment the DMZ basis the Risk appetite	DMZ shall be used for any Web hosting applica service like Terminal or Remote access (bastion bastion host) securely in a Uni-directio
			Cloud Network Access Control List	Network Access Control Lists (NACLs) act as firewalls for subnets within a Virtual Private Cloud (VPC), controlling traffic in and out of those subnets	One can also compliment NACL along with Ap Groups however not at the NIC Level since it's n Cloud model best practices
			Certificate Management	The process of acquiring, deploying, and managing Transport Layer Security (TLS) certificates within a cloud environment. This includes managing certificates for various cloud services like load balancers, proxies, and media CDNs	
		Data at Rest	Patch Management	Per SEBI Directives Patch Management falls under the purview of CSP	Patch Management varies basis the service m whether it is IaaS, PaaS, SaaS, Serverles
			System Level Vulnerability Management	Identifying Threats at the machine level on Cloud followed by Penetration Testing	
			System Hardening	**Though the system hardening is specified however there is no information on the same per circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023**	Approved Standards whether CIS benchmarks t other standards should have been s
			Server Side Encryption	**No information on the same per circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023**	SSE encrypts data on the serv

			Client Side Encryption	**No information on the same per circular SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033 dated March 06, 2023**	CSE encrypts data on the user's device befo
		Application Security	Source Code Review	Application source code review to identify vulnerabilities at the code level	Static Analysis (SAST) should have bee
			Web Application Testing	Dynamic application testing (DAST) coupled with Penetration	Threat Modelling basis principles of STR
					Security at the API level, Run time application se Serverless workload security (at the Functiona Security
2	Key Management	On-Premise KMS	On-Prem hosting of the key management system basis hardware deployed	Certificate(s) used for sessions at the application level could also be provisioned on the same device	
		Key Management as a Service	KMSaaS can be provisioned at the CSP level		
		Dedicated hardware Security Module	Dedicated HSM hosting at the CSP level		
3	Identity & Access Management	Individual Named User	User ID creation at the AD Level	PIM/PAM Integration at the AD level	
		Multifactor Authentication	2FA/Multifactor based authentication	specify attributes viz Geo Location, IP, Time	
		Programmatic Access	allows you to invoke actions on your CSP resources either through an application that you write or through a third-party tool	above attributes be coupled with delegated access viz CBAC, ABAC, RBAC	
		Temporary Credentials using Roles (JIT - Just in Time)	Standard JIT access at the CSP level	Standard Just in Time access at the User Level	mid tier service/bastion host based access via U from On-Prem/Hybrid to Clou
		Rotate Credentials/Password Policy	Rotate the credentails, password, keys		
		Access Rights Reviews	User access review for access delegated to individuals		
4	Log Management	Log Analysis (SIEM)	System Logs	Syslog provisioning	a. Syslog provisioning pointing at RTO, RPO p Compliance b. Specify log retention polic
			Network Traffic/VPC Flow logs	Perimeter, Network, VPC level logs for traffic be accumulated	Specify log retention policy
			DNS Logs	DNS logs for DNS Traffic from Internet to CSP Edge	a. log forwarding, log processing baselines & b. Provisioning of DNS SEC as a Techni
			User activity logs	User activity logs at the Technical Controls level, Application, DB Level be accumulated centrally in a sorted manner	Specify log retention policy

SEBI MINDMAP FOR CLOUD ADOPTION FRAMEWORK

		Log Retention & Archival	Log Retention & Archival Policy per SEBI Guidelines	This is line with the log retention policy per SEBI directives which is SEBI Requirements Trading records/transaction data: 5 years (minimum) KYC records: 5 years after the business relationship ends Stock broker records: 5 years (physical) and 8 years (electronic) Portfolio managers: 5 years Mutual fund transaction records: 8 years	SEBI Log Retention & Archival should have bee
		Continuous Monitoring & Alerting	Continuous monitoring & alert management system be considered	Continuous monitoring & alert management system through SIEM	
5	Cloud Security Policy Framework	Cloud Operational Procedures	Standard SOP's for Cloud enabled services	SOP's would ensure standards being followed	
		BCP/DR Framework, Test Procedures	Check the Cloud resilience for hosted applications/workload	maps the resilience at CSP, Application, Infra, Service level	Breach attack simulation
		Internal Audit	Internal audit to determine the compliance at Policy, Procedures, Guidelines basis benchmarks	Standard audit practices	
		Security Certification procedure before go live in Cloud	Standardization Testing and Quality Certification	STQC practices be invoked to ensure adequate testing	
		Mandatory Security Control Baseline	Security baseline for Security assessment at the Technical Control rendered on Cloud	Benchmarking be done	

Translation of the SEBI Cloud Controls into a Potential Architectural Diagram


Cloud Security Technical Architecture
Implementation of Comprehensive Cloud Security Controls
On-Premises Environment
Security Operations Center
SIEM Integration
Security Incident Management
Continuous Monitoring & Alerting
Identity Management
Active Directory / LDAP
Multi-Factor Authentication (MFA)
Identity Lifecycle Management
Security Management
Patch Management System
Vulnerability Management
On-premises KMS
Hardware Security Module (HSM)
System Hardening Guidelines
VPN
TLS
IdP
API
Secure Connectivity
Cloud Environment
Identity & Access Management
Federated Identity & SSO
Multi-Factor Authentication
Role-Based Access Control (RBAC)
Access Rights Review
Network Security
Cloud Network Access Control Lists
Web Application Firewall (WAF)
DDoS Protection
Data Security
Key Management Service (KMS)
Storage Encryption (Data at Rest)
Client-Side Encryption
Application Security
Code Review
App Testing
Cloud Security Policy Framework
Security Certification Procedures
BCP/DR Framework & Testing
Mandatory Security Baseline
Cloud Operational Procedures
Internal Audit Framework
Monitoring & Logging
Log Analysis (SIEM)
System Logs
Network Traffic/VPC Flow Logs
DNS Logs
User Activity Logs
Log Retention & Archival
Incident Response
Security Incident Management
Playbooks & Response Procedures
On-Premises
Cloud

Key Components of the Architecture

1. On-Premises Environment

Security Operations Centre (SOC)

- **SIEM Integration**: Central security event monitoring platform
- **Security Incident Management**: Processes for handling security incidents
- **Continuous Monitoring & Alerting**: Real-time threat detection systems

Identity Management

- **Active Directory/LDAP**: Central identity repository
- **Multi-Factor Authentication**: Additional authentication layer
- **Identity Lifecycle Management**: Manages user access throughout employment lifecycle

Security Management

- **Patch Management System**: Automated vulnerability remediation
- **Vulnerability Management**: Regular security scanning
- **On-premises KMS**: Key management for local systems
- **Hardware Security Module (HSM)**: Secure key storage
- **System Hardening Guidelines**: Standardized security configurations

2. Secure Connectivity Layer

Provides secure communication channels between on-premises and cloud environments:

- **IPSEC VPN**: For secure network-level connectivity
- **TLS/SSL**: For secure application-level traffic
- **Identity Federation**: For seamless authentication between environments
- **API Gateway**: For secure API communication

3. Cloud Environment

Identity & Access Management

- **Federated Identity & SSO**: Integration with on-premises identity systems
- **Multi-Factor Authentication**: Extends security to cloud resources
- **Role-Based Access Control**: Principle of least privilege
- **Access Rights Review**: Regular verification of permissions

Network Security

- **Cloud Network ACLs**: Virtual firewall for cloud resources
- **Web Application Firewall**: Protects against web-based attacks
- **DDoS Protection**: Mitigation for denial of service attacks

Data Security

- **Key Management Service**: Centralized key management in cloud
- **Storage Encryption**: Protects data at rest
- **Client-Side Encryption**: Additional protection layer

Application Security

- **Code Review**: Analysis for security vulnerabilities
- **App Testing**: Dynamic and static application security testing

4. Cloud Governance & Compliance

Cloud Security Policy Framework

- **Security Certification Procedures**: Pre-deployment security validation

- **BCP/DR Framework & Testing:** Business continuity and disaster recovery
- **Mandatory Security Baseline**: Minimum security requirements
- **Cloud Operational Procedures**: Day-to-day security operations
- **Internal Audit Framework**: Regular security assessments

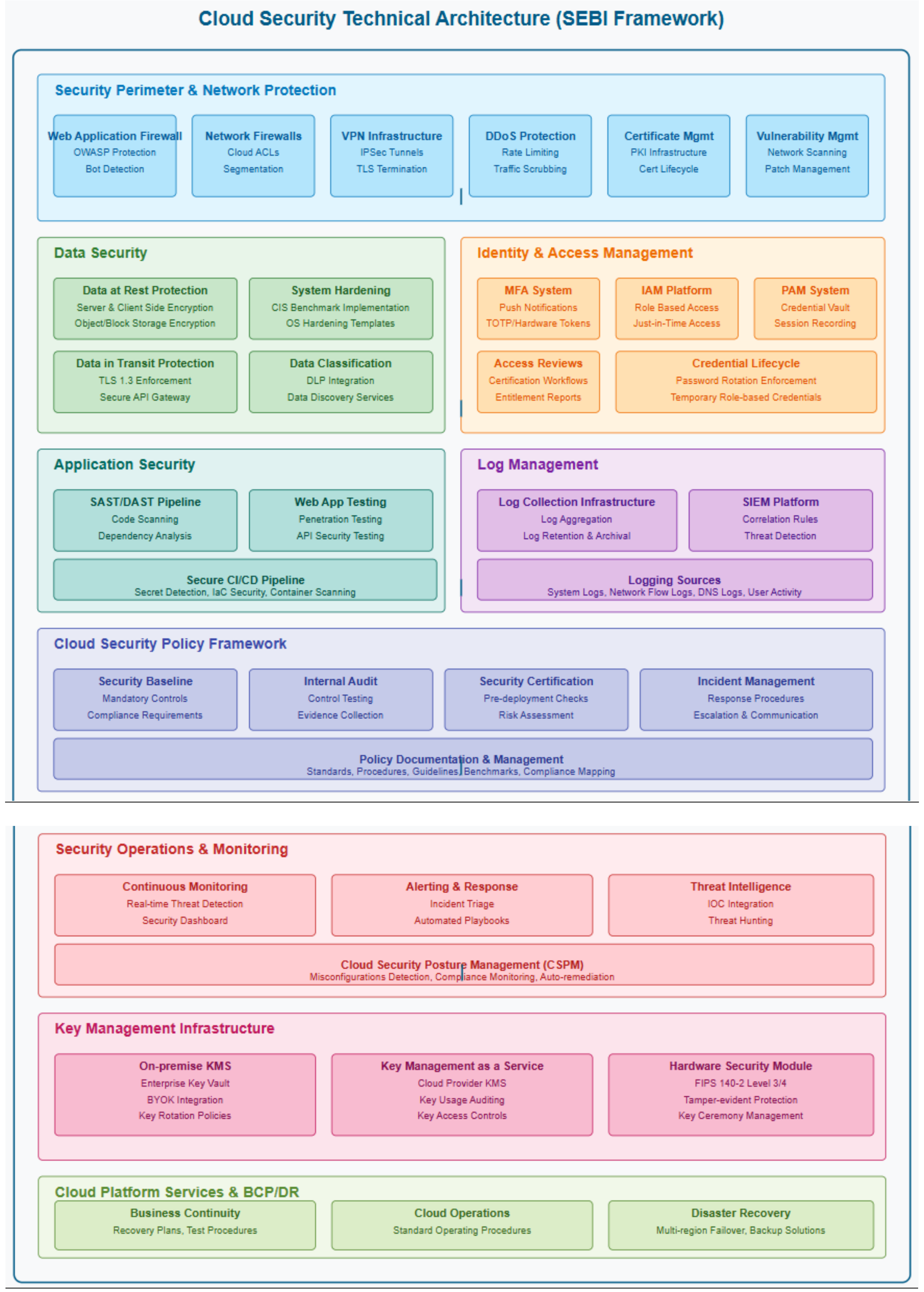
Monitoring & Logging

- **Log Analysis (SIEM):** Centralized log processing
- **System Logs**: Operating system and application events
- **Network Traffic/VPC Flow Logs**: Network activity monitoring
- **DNS Logs**: Domain resolution tracking
- **User Activity Logs**: User behaviour monitoring
- **Log Retention & Archival**: Long-term log preservation

Incident Response

- **Security Incident Management**: Structured incident handling
- **Playbooks & Response Procedures:** Standardized response actions

Creating a visionary Framework – what could have been better here ?



Cloud Security Technical Architecture (SEBI Framework)

Security Perimeter & Network Protection

- **Web Application Firewall**: OWASP Protection, Bot Detection
- **Network Firewalls**: Cloud ACLs, Segmentation
- **VPN Infrastructure**: IPSec Tunnels, TLS Termination
- **DDoS Protection**: Rate Limiting, Traffic Scrubbing
- **Certificate Mgmt**: PKI Infrastructure, Cert Lifecycle
- **Vulnerability Mgmt**: Network Scanning, Patch Management

Data Security

- **Data at Rest Protection**: Server & Client Side Encryption, Object/Block Storage Encryption
- **System Hardening**: CIS Benchmark Implementation, OS Hardening Templates
- **Data in Transit Protection**: TLS 1.3 Enforcement, Secure API Gateway
- **Data Classification**: DLP Integration, Data Discovery Services

Identity & Access Management

- **MFA System**: Push Notifications, TOTP/Hardware Tokens
- **IAM Platform**: Role Based Access, Just-in-Time Access
- **PAM System**: Credential Vault, Session Recording
- **Access Reviews**: Certification Workflows, Entitlement Reports
- **Credential Lifecycle**: Password Rotation Enforcement, Temporary Role-based Credentials

Application Security

- **SAST/DAST Pipeline**: Code Scanning, Dependency Analysis
- **Web App Testing**: Penetration Testing, API Security Testing
- **Secure CI/CD Pipeline**: Secret Detection, IaC Security, Container Scanning

Log Management

- **Log Collection Infrastructure**: Log Aggregation, Log Retention & Archival
- **SIEM Platform**: Correlation Rules, Threat Detection
- **Logging Sources**: System Logs, Network Flow Logs, DNS Logs, User Activity

Cloud Security Policy Framework

- **Security Baseline**: Mandatory Controls, Compliance Requirements
- **Internal Audit**: Control Testing, Evidence Collection
- **Security Certification**: Pre-deployment Checks, Risk Assessment
- **Incident Management**: Response Procedures, Escalation & Communication
- **Policy Documentation & Management**: Standards, Procedures, Guidelines, Benchmarks, Compliance Mapping

Security Operations & Monitoring

- **Continuous Monitoring**: Real-time Threat Detection, Security Dashboard
- **Alerting & Response**: Incident Triage, Automated Playbooks
- **Threat Intelligence**: IOC Integration, Threat Hunting
- **Cloud Security Posture Management (CSPM)**: Misconfigurations Detection, Compliance Monitoring, Auto-remediation

Key Management Infrastructure

- **On-premise KMS**: Enterprise Key Vault, BYOK Integration, Key Rotation Policies
- **Key Management as a Service**: Cloud Provider KMS, Key Usage Auditing, Key Access Controls
- **Hardware Security Module**: FIPS 140-2 Level 3/4, Tamper-evident Protection, Key Ceremony Management

Cloud Platform Services & BCP/DR

- **Business Continuity**: Recovery Plans, Test Procedures
- **Cloud Operations**: Standard Operating Procedures
- **Disaster Recovery**: Multi-region Failover, Backup Solutions

An Ideal list of Technical Control sets for Cloud Security

Low-Level Cloud Security Architecture Based on SEBI Framework

1. Core Infrastructure Components

1.1 Security Operations Centre (SOC)

- Central Security Monitoring Platform
  - SIEM Integration Hub
  - Correlation Engine
  - Threat Intelligence Feed Integration
  - Automated Alert Triage System
- Incident Response Automation
  - Playbook Execution Engine
  - Case Management System
  - Threat Containment Automation
- SOC Dashboard
  - Real-time Threat Visualization
  - Compliance Status Monitoring
  - Security Posture Indicators

1.2 Identity Management Infrastructure

- Identity Provider (IdP)
  - Central Authentication Service
  - Federation Service
  - Directory Services (LDAP/AD)
- Privileged Access Management (PAM)
  - Privileged Credential Vault
  - Just-in-Time Access Provisioning
  - Session Recording & Auditing
- MFA Infrastructure
  - Authentication Factor Management
  - Token Distribution System

  - Biometric Integration Services

1.3 Data Protection Infrastructure

- Key Management Service (KMS)
  - Hardware Security Module (HSM) Integration
  - Cryptographic Key Lifecycle Management
  - Key Rotation Automation
- Data Loss Prevention (DLP)
  - Content Inspection Engine
  - Policy Enforcement Points
  - Data Classification Service
- Encryption Service Mesh
  - TLS Termination Points
  - Certificate Management System
  - Transport Encryption Gateways

2. Network Security Layer

2.1 Perimeter Protection

- Cloud-Native Firewall Services
  - Layer 7 Application Filtering
  - Geo-IP Blocking
  - Rate Limiting & DDoS Protection
- Zero Trust Network Access (ZTNA)
  - Software-Defined Perimeter
  - Micro-segmentation Controllers
  - Continuous Trust Verification
- API Gateway & Security
  - API Authentication Service
  - Request Throttling
  - Payload Validation

2.2 Network Connectivity

- VPN Infrastructure
  - IPSec Tunneling Service

  - Split Tunnelling Controls
  - Site-to-Site Connection Manager
- Transit Gateway/Hub
  - Cross-VPC/VNET Routing
  - Traffic Inspection Points
  - Network Segmentation Controls
- Private Link Services
  - Service Endpoint Management
  - Private DNS Integration
  - Managed NAT Services

2.3 Network Monitoring

- Flow Log Collection
  - VPC/VNET Flow Aggregators
  - Traffic Pattern Analysis
  - Network Behavior Analytics
- Network IDS/IPS
  - Deep Packet Inspection
  - Signature-based Detection
  - Protocol Anomaly Detection
- DNS Security Monitoring
  - DNS Query Analytics
  - Domain Reputation Filtering
  - DNS Exfiltration Detection

3. Data Security Layer

3.1 Data Storage Security

- Encrypted Storage Services
  - Object Storage Encryption
  - Block Storage Encryption
  - Database Transparent Encryption
- Data Access Control
  - Fine-grained Access Policies

  - Attribute-based Access Control
  - Storage Access Analyzers
- Data Lifecycle Management
  - Retention Policy Enforcement
  - Secure Data Deletion
  - Version Control & Immutability

3.2 Data in Transit Protection

- TLS Management Service
  - Certificate Lifecycle Automation
  - Cipher Suite Policy Enforcement
  - Certificate Transparency Monitoring
- Secure Data Transfer
  - Data Transfer Nodes
  - Encryption Proxy Services
  - Transfer Activity Logging
- Network Encryption Overlay
  - IPsec Implementation
  - Key Exchange Services
  - Encrypted Routing Mesh

3.3 Data Classification & Governance

- Data Discovery Service
  - Automated Data Classification
  - Sensitive Data Scanner
  - Data Mapping & Inventory
- Data Access Governance
  - Entitlement Review System
  - Compliance Rule Engine
  - Data Access Reporting
- Data Sovereignty Controls
  - Geo-fencing Services
  - Data Residency Management

  - Cross-border Transfer Controls

4. Application Security Layer

4.1 Application Protection

- Web Application Firewall (WAF)
  - OWASP Rule Sets
  - Custom Rule Management
  - Bot Protection
- Runtime Application Self-Protection (RASP)
  - Code Execution Monitoring
  - Runtime Vulnerability Shielding
  - Attack Vector Neutralization
- API Security Gateway
  - Schema Validation
  - OAuth/JWT Token Validation
  - API Rate Limiting

4.2 Secure Development Pipeline

- Code Security Scanning
  - Static Application Security Testing (SAST)
  - Software Composition Analysis (SCA)
  - Secret Detection Service
- Container Security
  - Image Scanning Service
  - Registry Security Controls
  - Runtime Container Monitoring
- Infrastructure as Code (IaC) Security
  - Template Scanning
  - Compliance as Code Validation
  - Security Policy as Code

4.3 Application Testing

- Dynamic Application Security Testing
  - Automated Vulnerability Scanning

  - Penetration Testing Orchestration
  - Fuzz Testing Services
- API Security Testing
  - API Contract Validation
  - API Abuse Testing
  - API Authentication Testing
- Dependency Vulnerability Management
  - Dependency Graph Analysis
  - Vulnerability Database Integration
  - Remediation Workflow

5. Identity and Access Management

5.1 User Identity Management

- User Lifecycle Management
  - Onboarding/Offboarding Automation
  - Identity Governance
  - Access Certification
- Authentication Services
  - MFA Orchestration
  - Adaptive Authentication
  - Single Sign-On Service
- Directory Services
  - User Repository
  - Group Management
  - Organizational Structure

5.2 Access Control

- Role-based Access Control (RBAC)
  - Role Definition Repository
  - Role Assignment Service
  - Role Hierarchy Management
- Attribute-based Access Control (ABAC)
  - Policy Decision Points

  - Policy Information Points
  - Context-aware Access Rules
- Just-in-Time Access
  - Access Request Workflow
  - Approval Chain Automation
  - Time-bound Credential Issuance

5.3 Credential Management

- Secrets Management
  - Application Credential Vault
  - Dynamic Secret Generation
  - Secret Rotation Service
- Password Management
  - Password Policy Enforcement
  - Self-service Password Reset
  - Password Strength Validation
- Certificate Management
  - Certificate Authority Integration
  - Certificate Lifecycle Automation
  - Certificate Expiry Monitoring

6. Governance, Risk and Compliance

6.1 Policy Management

- Policy Administration
  - Policy Repository
  - Policy Distribution
  - Policy Version Control
- Security Baseline Management
  - Baseline Configuration Templates
  - Baseline Compliance Monitoring
  - Remediation Workflow
- Regulatory Mapping
  - Control Mapping Repository

  - Compliance Framework Correlation
  - Audit Evidence Collection

6.2 Risk Management

- Risk Assessment
  - Asset Inventory Service
  - Vulnerability Management System
  - Threat Modelling Automation
- Risk Treatment
  - Risk Mitigation Planning
  - Risk Acceptance Workflow
  - Compensating Control Management
- Risk Monitoring
  - Key Risk Indicators
  - Risk Dashboard
  - Risk Trend Analysis

6.3 Audit & Compliance

- Audit Logging
  - Centralized Log Collection
  - Log Integrity Protection
  - Log Retention Management
- Compliance Monitoring
  - Continuous Compliance Checks
  - Compliance Scoring
  - Control Effectiveness Measurement
- Audit Readiness
  - Evidence Collection Automation
  - Audit Trail Management
  - Audit Response Workflow

7. Security Operations

7.1 Vulnerability Management

- Vulnerability Scanning

    - Cloud Resource Scanners
    - Configuration Assessment
    - Vulnerability Correlation
- Patch Management
    - Patch Assessment
    - Patching Orchestration
    - Patch Compliance Monitoring
- System Hardening
    - Hardening Templates
    - Drift Detection
    - Configuration Enforcement

7.2 Threat Detection

- Threat Intelligence
    - Threat Feed Integration
    - IOC Management
    - Threat Hunting Platform
- Behavioral Analytics
    - User Behavior Analytics (UBA)
    - Entity Behavior Analytics
    - Anomaly Detection
- Alert Management
    - Alert Correlation
    - Alert Prioritization
    - Alert Routing & Escalation

7.3 Incident Response

- Incident Management
    - Incident Classification
    - Incident Tracking System
    - Post-Incident Analysis
- Response Automation
    - Automated Containment

  - Evidence Collection
  - Forensic Analysis Tools
- Crisis Management
  - Communication Channels
  - Stakeholder Notification
  - Business Continuity Integration

8. Business Continuity & Disaster Recovery

8.1 Backup Management

- Backup Services
  - Automated Backup Scheduling
  - Backup Verification Testing
  - Retention Management
- Data Recovery
  - Point-in-time Recovery
  - Cross-region Recovery
  - Recovery Testing Automation
- Immutable Backups
  - WORM Storage Integration
  - Backup Encryption
  - Backup Access Controls

8.2 Disaster Recovery

- DR Planning
  - DR Strategy Definition
  - Recovery Objective Management
  - DR Documentation System
- DR Testing
  - DR Drill Orchestration
  - Recovery Time Measurement
  - Test Result Analysis
- DR Automation
  - Failover Automation

  - DR Runbooks
  - Cross-region Replication

8.3 Resilience Engineering

- Chaos Engineering
  - Controlled Failure Injection
  - Resilience Testing Framework
  - Service Degradation Simulation
- High Availability Design
  - Multi-AZ Deployment Management
  - Load Balancing Configuration
  - Health Check Management
- Service Mesh Resilience
  - Circuit Breaking Implementation
  - Retry/Timeout Management
  - Traffic Shifting Controls

9. Cloud Security Posture Management

9.1 Cloud Configuration Monitoring

- Cloud Security Posture Management
  - Misconfigurations Detection
  - Best Practice Validation
  - Automated Remediation
- Infrastructure Monitoring
  - Resource Configuration Assessment
  - Security Group Analysis
  - Identity Permission Review
- Service Usage Monitoring
  - Shadow IT Detection
  - Service Entitlement Management
  - Resource Tagging Compliance

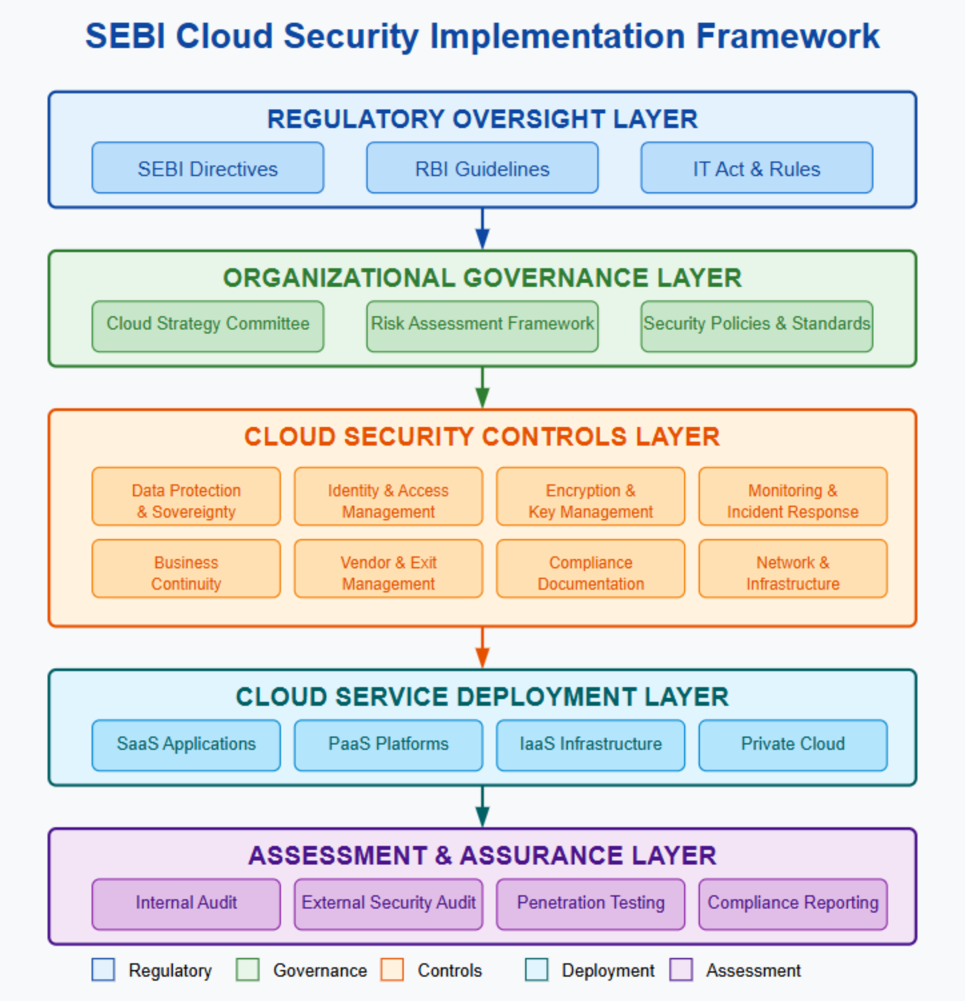
9.2 Cloud Workload Protection

- Server Protection

  - Host-based Intrusion Detection
  - File Integrity Monitoring
  - Runtime Protection
- Container Security
  - Container Runtime Monitoring
  - Orchestrator Security Controls
  - Container Network Policy Enforcement
- Serverless Security
  - Function Configuration Scanning
  - Function Runtime Monitoring
  - Event Source Security

9.3 Cloud Native Security Controls

- Native Security Services Integration
  - Cloud Provider Security API Integration
  - Security Service Orchestration
  - Cross-cloud Security Normalization
- Security Automation
  - Infrastructure as Code Security Checks
  - Security as Code Implementation
  - Automated Remediation Workflows
- Cloud Security Benchmarks
  - CIS Benchmark Implementation
  - Industry Standard Alignment
  - Security Score Calculation


SEBI Cloud Security Implementation Framework
REGULATORY OVERSIGHT LAYER
SEBI Directives
RBI Guidelines
IT Act & Rules
ORGANIZATIONAL GOVERNANCE LAYER
Cloud Strategy Committee
Risk Assessment Framework
Security Policies & Standards
CLOUD SECURITY CONTROLS LAYER
Data Protection & Sovereignty
Identity & Access Management
Encryption & Key Management
Monitoring & Incident Response
Business Continuity
Vendor & Exit Management
Compliance Documentation
Network & Infrastructure
CLOUD SERVICE DEPLOYMENT LAYER
SaaS Applications
PaaS Platforms
IaaS Infrastructure
Private Cloud
ASSESSMENT & ASSURANCE LAYER
Internal Audit
External Security Audit
Penetration Testing
Compliance Reporting
□ Regulatory
□ Governance
□ Controls
□ Deployment
□ Assessment

SEBI Cloud Security Policy Framework: High Level Analysis

Key Framework Components

The SEBI cloud security framework is organized in a layered approach:

1. **Regulatory Oversight Layer** - SEBI directives, RBI guidelines, and IT Act requirements that govern cloud adoption
2. **Organizational Governance Layer** - Internal committees and policies that manage cloud strategy
3. **Cloud Security Controls Layer** - Specific security measures required for cloud deployments
4. **Cloud Service Deployment Layer** - Various cloud models (SaaS, PaaS, IaaS) with their security requirements
5. **Assessment & Assurance Layer** - Continuous monitoring and verification mechanisms

Implementation Mandates

Each component of the framework comes with specific implementation requirements, including:

- Establishing cloud governance committees with cross-functional representation
- Conducting thorough risk assessments before cloud migrations

- Implementing data classification and protection controls
- Ensuring strong identity and access management with MFA
- Maintaining comprehensive encryption and key management practices
- Establishing continuous monitoring and incident response capabilities
- Creating detailed business continuity and disaster recovery plans
- Managing third-party risks throughout the cloud supply chain
- Ensuring legal and regulatory compliance