Contents

Cloud Security Governance Framework

Comprehensive Technical Report

Document Version: 1.0
Date: November 29, 2025
Classification: Confidential - Internal Use
Author: Enterprise Security Team

GitHub Repository:
https://github.com/jeffmakuto/deep-learning/tree/master/cloud_security_governance

---

Table of Contents

---

1. Introduction

1.1 Executive Overview

This document presents a comprehensive security governance framework designed for a medium-sized enterprise transitioning to cloud infrastructure. The framework addresses the unique security challenges of cloud computing while ensuring regulatory compliance with GDPR, HIPAA, and CCPA requirements.

1.2 Business Context

Organization Profile: - Size: 500-2,000 employees - Revenue: $50M-$500M annually - Customer base: 100K+ customers with sensitive data - Geographic presence: North America, Europe - Industry: Healthcare, Financial Services, or Technology

Cloud Migration Drivers: - Cost optimization (30-40% infrastructure savings) - Scalability and flexibility - Innovation and agility - Global reach and performance - Disaster recovery capabilities

Data Classification: - **Critical:** PHI, PII, financial records (30% of data) - **Confidential:** Business intelligence, trade secrets (40% of data) - **Internal:** Employee data, communications (25% of data) - **Public:** Marketing materials, public documentation (5% of data)

1.3 Cloud Strategy

Multi-Cloud Approach: - **AWS:** Primary platform (60% workloads) - Production applications - **Azure:** Secondary platform (30% workloads) - Microsoft ecosystem integration - **Google Cloud:** Tertiary platform (10% workloads) - Data analytics, ML

Migration Phases: - Phase 1: Non-production environments (Completed) - Phase 2: Low-risk production workloads (Current) - Phase 3: Business-critical applications (Next 6 months) - Phase 4: Highly regulated workloads (12-18 months)

1.4 Framework Objectives

1. **Security First:** Implement defense-in-depth across all cloud layers
2. **Compliance Assurance:** Maintain continuous regulatory compliance
3. **Risk Management:** Proactive threat identification and mitigation
4. **Business Enablement:** Secure cloud adoption without innovation barriers
5. **Operational Excellence:** 24/7 security operations and monitoring
6. **Continuous Improvement:** Regular assessment and framework evolution

---

2. Risk Assessment

2.1 Risk Assessment Methodology

Framework: NIST Risk Management Framework (RMF) + ISO 27005

Risk Scoring Formula:

```
Risk Score = Likelihood (1-5) × Impact (1-5) × Exposure Factor (1-3)
Risk Level:
- Critical: 50-75
- High: 25-49
- Medium: 10-24
- Low: 1-9
```

Assessment Frequency: - Comprehensive assessment: Annually - Targeted assessment: Quarterly - Continuous monitoring: Real-time - Post-incident assessment: As needed

2.2 Technical Vulnerabilities

2.2.1 Cloud Misconfigurations Risk Score: 45 (High)

Common Misconfigurations:

Misconfiguration	Prevalence	Impact	Detection Method
Open S3 buckets	Very High	Critical	AWS Config, CSPM
Overly permissive IAM	High	High	IAM Access Analyzer

Misconfiguration	Prevalence	Impact	Detection Method
Unencrypted storage	Medium	Critical	AWS Inspector
Public RDS instances	Medium	Critical	Security Hub
Missing security groups	High	High	VPC Flow Logs
Disabled logging	Medium	High	CloudTrail analysis

Mitigation Strategies: - **Preventive Controls:** - Infrastructure as Code (IaC) with security scanning - AWS Service Control Policies (SCPs) - Azure Policy enforcement - Automated compliance checks in CI/CD

- **Detective Controls:**
  - Cloud Security Posture Management (CSPM) - Prisma Cloud, Wiz
  - Continuous configuration monitoring
  - Daily compliance scans
  - Real-time alerting on drift
- **Corrective Controls:**
  - Automated remediation (Lambda, Azure Functions)
  - Configuration management tools (Terraform, CloudFormation)
  - Rollback capabilities
  - Change approval workflow

Example: S3 Bucket Hardening

```
{
  "S3BucketPolicy": {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "DenyInsecureTransport",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::sensitive-data-bucket/*",
        "Condition": {
          "Bool": {"aws:SecureTransport": "false"}
        }
      },
      {
        "Sid": "DenyUnencryptedObjectUploads",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::sensitive-data-bucket/*",
        "Condition": {
          "StringNotEquals": {
            "s3:x-amz-server-side-encryption": "aws:kms"
          }
        }
      }
    ]
  }
}
```

2.2.2 API Security Vulnerabilities Risk Score: 38 (High)

Vulnerability Categories: - **Authentication Bypass:** Weak or missing API authentication - **Broken Object Level Authorization:** Accessing unauthorized resources - **Excessive Data Exposure:** APIs returning more data than necessary - **Rate Limiting:** Missing or insufficient rate limiting - **Injection Attacks:** SQL, NoSQL, command injection - **Security Misconfiguration:** Default credentials, verbose errors

Mitigation Strategies: - API Gateway with authentication (AWS API Gateway, Azure APIM) - OAuth 2.0 / OpenID Connect for authorization - API key rotation every 90 days - Rate limiting: 1000 requests/minute per user - Input validation and output encoding - API security testing in CI/CD (OWASP ZAP, Burp Suite) - API threat monitoring (Wallarm, Salt Security)

2.2.3 Data Encryption Gaps Risk Score: 42 (High)

Encryption Requirements:

Data State	Encryption Standard	Key Management	Compliance
At-Rest	AES-256	AWS KMS, Azure Key Vault	REQUIRED
In-Transit	TLS 1.3	Certificate Manager	REQUIRED
In-Use	Application-level	HashiCorp Vault	RECOMMENDED
Backups	AES-256	Dedicated backup keys	REQUIRED
Logs	AES-256	CloudWatch encryption	REQUIRED

Key Management Best Practices: - Separate keys per environment (dev, staging, prod) - Automatic key rotation every 90 days - Customer Managed Keys (CMK) for sensitive data - Multi-region key replication for DR - Key usage auditing via CloudTrail - Hardware Security Module (HSM) for payment data

2.2.4 Network Security Weaknesses Risk Score: 35 (High)

Network Architecture Security:

```
Internet
    ↓
AWS WAF / Azure Firewall
    ↓
Application Load Balancer (Public Subnet)
    ↓
Application Tier (Private Subnet)
    ↓
Database Tier (Private Subnet - No Internet)
    ↓
VPC Peering / Private Link for inter-VPC
```

Security Controls: - Network segmentation (VPC, subnets, security groups) - Web Application Firewall (WAF) for OWASP Top 10 - DDoS protection (AWS Shield Advanced, Azure DDoS) - Network ACLs for subnet-level filtering - VPC Flow Logs for traffic analysis - Private endpoints for AWS/Azure services - Bastion hosts with MFA for administrative access

2.3 Human Factor Risks

2.3.1 Insider Threats Risk Score: 48 (High)

Threat Categories:

Insider Type	Motivation	Prevalence	Impact
Malicious Insider	Financial gain, revenge	15%	Critical
Negligent Insider	Carelessness, shortcuts	60%	High
Compromised Insider	Account takeover	20%	Critical
Third-Party Insider	Vendor employee	5%	High

Detection & Prevention:

User and Entity Behavior Analytics (UEBA): - Baseline normal behavior patterns - Detect anomalies: unusual access times, data exfiltration - Risk scoring per user/entity - Tools: AWS Detective, Azure Sentinel UEBA, Splunk UBA

Data Loss Prevention (DLP): - Monitor sensitive data movement - Block unauthorized transfers (email, USB, cloud) - Endpoint DLP + Cloud DLP - Tools: Microsoft Purview, Symantec DLP, Forcepoint

Access Controls: - Least privilege principle (POLP) - Just-in-Time (JIT) access - Privileged Access Management (PAM) - Separation of duties (SoD) - Regular access reviews (quarterly)

Monitoring: - CloudTrail/Azure Activity Logs for all API calls - Database access monitoring (AWS RDS Enhanced Monitoring) - File integrity monitoring (FIM) - Session recording for privileged users

Example Insider Threat Scenario:

```
Alert: DevOps engineer accessing production database at 2 AM
→ UEBA flags as anomalous (normal hours 9 AM - 6 PM)
→ Session recorded via PAM
→ Security team investigates
→ Legitimate on-call activity confirmed
→ Future 2 AM access from same user = normal baseline updated
```

2.3.2 Phishing & Social Engineering Risk Score: 40 (High)

Attack Vectors: - Email phishing (95% of attacks) - Spear phishing (targeted executives) - Smishing (SMS phishing) - Vishing (voice phishing) - Business Email Compromise (BEC)

Defense Strategies:

Technical Controls: - Email security gateway (Proofpoint, Mimecast) - DMARC, SPF, DKIM authentication - Link sandboxing and URL rewriting - Attachment sandboxing - Phishing simulation tools (KnowBe4, Cofense)

Security Awareness Training: - Monthly phishing simulations - Quarterly security training modules - Annual comprehensive training - Role-based training (executives, developers, finance) - Reporting mechanism for suspicious emails - Gamification and rewards for vigilant reporting

Metrics: - Phishing click rate: Current 12% → Target $< 5\%$ - Reporting rate: Current 8% → Target $> 50\%$ - Training completion: 100% required

2.3.3 Insufficient Training & Awareness Risk Score: 32 (Medium-High)

Knowledge Gaps: - Cloud security best practices (60% of staff) - Data classification and handling (45% of staff) - Incident reporting procedures (35% of staff) - Secure coding practices (50% of developers) - Regulatory compliance requirements (40% of staff)

Training Program:

Audience	Training Type	Frequency	Duration
All Employees	Security Awareness	Annually	2 hours
Developers	Secure Coding	Quarterly	4 hours
Cloud Engineers	Cloud Security	Bi-annually	8 hours
Executives	Cyber Risk Management	Annually	2 hours
Security Team	Advanced Security	Monthly	Varies

Certifications Encouraged: - AWS Certified Security - Specialty - Microsoft Certified: Azure Security Engineer - Google Professional Cloud Security Engineer - CISSP, CISM, CEH - SANS GIAC certifications

2.4 Third-Party Risks

2.4.1 Vendor Security Posture Risk Score: 35 (High)

Critical Vendors: - Cloud providers (AWS, Azure, Google Cloud) - SaaS applications (CRM, HR, collaboration) - Managed security service providers (MSSP) - Payment processors - Data analytics platforms

Vendor Risk Management Process:

1. Pre-Contract Assessment: - Security questionnaire (SIG Lite, CAIQ) - SOC 2 Type II report review - ISO 27001 certification verification - Penetration testing results - Incident history disclosure - Financial stability check

2. Contract Requirements: - Security SLA (99.9% uptime, MTTD/MTTR) - Data Processing Agreement (DPA) for GDPR - Business Associate Agreement (BAA) for HIPAA - Right to audit clause - Data encryption requirements - Breach notification timeline (< 24 hours) - Liability and indemnification terms

3. Ongoing Monitoring: - Annual SOC 2 recertification - Quarterly security posture reviews - Continuous monitoring (SecurityScorecard, BitSight) - Vendor access reviews - Exit strategy and data portability

4. **Vendor Tiers:** - **Tier 1 (Critical):** Full assessment, annual audit, dedicated account manager - **Tier 2 (High):** Standard assessment, SOC 2 required - **Tier 3 (Medium):** Questionnaire, certifications preferred - **Tier 4 (Low):** Basic due diligence

2.4.2 Supply Chain Security Risk Score: 38 (High)

Attack Vectors: - Compromised software dependencies (npm, PyPI) - Trojanized firmware/hardware - Malicious code injection in CI/CD pipeline - Compromised cloud service provider

Mitigation: - Software Bill of Materials (SBOM) for all applications - Dependency scanning (Snyk, Dependabot) - Code signing and verification - Secure CI/CD pipeline (hardened Jenkins, GitLab) - Network segmentation for vendor access - Least privilege for third-party integrations

Example: Open Source Dependency Management

```
# Automated dependency scanning in CI/CD
security-scan:
  stage: test
  script:
    - snyk test --severity-threshold=high
    - npm audit --audit-level=moderate
    - owasp-dependency-check --project myapp
  allow_failure: false  # Block deployment on critical vulnerabilities
```

2.5 Cloud-Specific Risks

2.5.1 Shared Responsibility Confusion Risk Score: 30 (Medium-High)

Shared Responsibility Model:

```
Customer Responsibility ("Security IN the Cloud")
   Data classification and encryption
   Application security and patching
   Identity and access management
   Network controls (security groups, NACLs)
   Operating system and database patching (EC2, RDS)

Cloud Provider Responsibility ("Security OF the Cloud")
   Physical data center security
   Network infrastructure
   Hypervisor security
   Managed service patching (Lambda, S3, RDS managed)
   Hardware and firmware maintenance
```

Clarity Mechanisms: - Documented responsibility matrix - Regular training on shared responsibility - Automated compliance checks for customer controls - Vendor security documentation review

2.5.2 Multi-Tenancy Risks Risk Score: 25 (Medium)

Concerns: - Data leakage between tenants - Resource exhaustion attacks - Side-channel attacks - Hypervisor escape vulnerabilities

Mitigation: - Dedicated instances for highly sensitive workloads - Encryption with customer-managed keys - Regular vulnerability assessments - Compliance with cloud security benchmarks (CIS) - Monitoring for anomalous resource usage

2.5.3 Data Residency & Sovereignty Risk Score: 28 (Medium-High)

Regulatory Requirements: - **GDPR:** EU data must remain in EU (or adequate country) - **HIPAA:** No specific residency requirement, but BAA required - **CCPA:** No specific residency requirement

Controls: - Region selection based on data classification - Data residency policies in IaC - Cross-region replication controls - Legal review for cross-border transfers - Standard Contractual Clauses (SCCs) for EU transfers

2.6 Risk Register Summary

Top 20 Risks (Prioritized):

Rank	Risk	Risk Score	Priority	Owner
1	Insider threat - data exfiltration	48	P1	CISO
2	Cloud misconfiguration - public exposure	45	P1	Cloud Security Engineer
3	Data encryption gaps	42	P1	Cloud Security Engineer
4	Phishing/social engineering	40	P1	Security Awareness Lead
5	API security vulnerabilities	38	P2	Application Security
6	Supply chain compromise	38	P2	Vendor Risk Manager
7	Third-party vendor breach	35	P2	Vendor Risk Manager
8	Network security weaknesses	35	P2	Network Security Engineer
9	Insufficient security training	32	P2	CISO

Rank	Risk	Risk Score	Priority	Owner
10	Shared responsibility confusion	30	P3	Compliance Officer
11	Data residency violations	28	P3	Compliance Officer
12	Multi-tenancy risks	25	P3	Cloud Security Engineer
13	DDoS attacks	24	P3	Network Security Engineer
14	Ransomware	42	P1	SOC Manager
15	Privilege escalation	35	P2	IAM Administrator
16	Compliance violations	40	P1	Compliance Officer
17	Lack of visibility in cloud	32	P2	SOC Manager
18	Inadequate incident response	38	P2	Incident Response Lead
19	Business continuity gaps	35	P2	DR Manager
20	Shadow IT and unapproved cloud use	28	P3	CISO

---

3. Security Policies & Procedures

3.1 Policy Framework

Policy Hierarchy:

```
Corporate Security Policy (Board-approved)
    ↓
Domain-Specific Policies (CISO-approved)
       Data Protection Policy
       Access Control Policy
       Encryption Policy
       Incident Response Policy
       Acceptable Use Policy
       Change Management Policy
       Third-Party Security Policy
    ↓
Standards & Guidelines (Cloud Security Engineer-approved)
       AWS Security Standards
       Azure Security Standards
       Google Cloud Security Standards
       Secure Coding Standards
    ↓
Procedures (Department Lead-approved)
       Cloud Configuration Procedures
       Access Provisioning Procedures
       Incident Handling Procedures
       Audit Procedures
```

Policy Lifecycle: - **Development:** 4-6 weeks, stakeholder input - **Approval:** CISO → Legal → Board (for corporate policy) - **Communication:** All-hands, email, intranet - **Training:** Mandatory acknowledgment - **Review:** Annual or upon significant change - **Updates:** Version control, change log

3.2 Data Protection Policy

Policy Statement: All organizational data must be classified, protected, and handled according to its sensitivity level to prevent unauthorized disclosure, modification, or destruction.

Data Classification:

Classification	Definition	Examples	Protection Requirements
Critical	Data that if compromised would have catastrophic impact	PHI, SSN, credit cards, encryption keys	AES-256, access logging, DLP, MFA
Confidential	Data that if disclosed would have significant impact	Trade secrets, financial data, customer lists	AES-256, access controls, encryption in transit
Internal	Data for internal use only	Employee directories, internal communications	Encryption in transit, authentication
Public	Data approved for public disclosure	Marketing materials, press releases	No special protection

Data Handling Requirements:

Storage: - Critical/Confidential: Encrypted at rest (AES-256), dedicated encryption keys - Internal: Encrypted at rest (provider-managed keys acceptable) - Public: No encryption required, but recommended

Transmission: - All data: TLS 1.3 for external, TLS 1.2 minimum for internal - Critical: Additional application-layer encryption for highly sensitive fields

Processing: - Critical: Tokenization or encryption in applications - Confidential: Secure coding practices, input validation - Logging: No sensitive data in logs (use masking/redaction)

Retention: - Critical: 7 years (HIPAA, financial regulations) - Confidential: 5 years or per legal hold - Internal: 3 years - Public: No retention requirement

Disposal: - Critical/Confidential: Secure deletion (cryptographic erasure, DoD 5220.22-M) - Cloud storage: Delete + versioning removal + backup purge - Physical media: Shred or degauss

Data Protection Procedures: See Data Protection Procedures for detailed implementation steps.

3.3 Access Control Policy

Policy Statement: Access to information systems and data shall be granted based on the principle of least privilege, authenticated through multi-factor methods, and regularly reviewed for appropriateness.

Access Control Model: Role-Based Access Control (RBAC)

Core Roles:

Role	Permissions	MFA Required	Review Frequency
Cloud Administrator	Full AWS/Azure admin	Yes (hardware token)	Quarterly
Database Administrator	Database read/write, backup	Yes (hardware token)	Quarterly
Developer	Code repo, dev/staging environment	Yes (software token)	Bi-annually
Security Analyst	Read-only security logs, SIEM	Yes (software token)	Bi-annually
End User	Email, collaboration tools	Yes (SMS/app)	Annually
Auditor	Read-only audit logs	Yes (software token)	Per audit

Access Request Process: 1. Employee submits access request via IT ticketing system 2. Manager approval required 3. Security team reviews and approves (24-hour SLA) 4. Access provisioned with least privilege 5. Automated notification to user and manager 6. Access logged in IAM system

Just-in-Time (JIT) Access: - Privileged access granted for limited time (4 hours max) - Break-glass accounts for emergencies - All JIT access logged and reviewed

Multi-Factor Authentication (MFA): - Mandatory for: - All cloud console access - VPN access - Privileged accounts - Email access from untrusted networks

- **MFA Methods (in order of preference):**
  1. Hardware token (YubiKey) - For administrators
  2. Software authenticator app (Duo, Okta Verify) - For standard users
  3. SMS (least preferred, only for low-risk systems)

Access Reviews: - Automated quarterly reports to managers - Manager certifies access is appropriate - Security team spot-checks 10% of access - Orphaned accounts disabled after 90 days of inactivity

Privileged Access Management (PAM): - Centralized password vault (CyberArk, BeyondTrust) - Session recording for all privileged sessions - Automatic password rotation every 90 days - Check-out/check-in for shared accounts

Access Control Procedures: See Access Management Procedures

3.4 Encryption Policy

Policy Statement: All sensitive data must be encrypted at rest and in transit using industry-standard encryption algorithms and key management practices.

Encryption Standards:

Symmetric Encryption: - Algorithm: AES-256 - Mode: GCM (Galois/Counter Mode) for authenticated encryption - Use cases: Data at rest, bulk encryption

Asymmetric Encryption: - Algorithm: RSA 4096-bit or ECC P-384 - Use cases: Key exchange, digital signatures

Hashing: - Algorithm: SHA-256 or SHA-3 - Password hashing: bcrypt, scrypt, or Argon2 - Use cases: Data integrity, password storage

Key Management:

Key Lifecycle:

```
Key Generation → Key Distribution → Key Storage → Key Usage → Key Rotation → Key Archival → Key
```

Key Hierarchy:

```
Master Key (HSM-protected, rotated annually)
    ↓
Data Encryption Keys (DEK) (rotated quarterly)
    ↓
Encrypted Data
```

Key Storage: - **AWS:** AWS Key Management Service (KMS) with HSM backing - **Azure:** Azure Key Vault with Premium (HSM) tier - **Google Cloud:** Cloud KMS with HSM protection - **Secrets:** HashiCorp Vault for application secrets, API keys

Key Rotation: - Master keys: Annually - Data encryption keys: Quarterly - Application secrets: Every 90 days - SSH keys: Every 180 days - TLS certificates: Annually or per CA requirements

Encryption at Rest:

Data Type	Encryption Method	Key Type	Rotation
Database (RDS)	Transparent Data Encryption (TDE)	AWS KMS CMK	Quarterly
Object storage (S3)	SSE-KMS	AWS KMS CMK	Quarterly
File storage (EFS)	Native encryption	AWS KMS CMK	Quarterly
Backups	Encrypted snapshots	Dedicated backup keys	Quarterly
Application data	Application-level	App-specific keys	Quarterly
Logs	CloudWatch Encryption	AWS KMS CMK	Quarterly

Encryption in Transit:

Connection Type	Protocol	Certificate	Configuration
Web traffic (external)	TLS 1.3	Public CA cert	Perfect Forward Secrecy
Web traffic (internal)	TLS 1.2+	Internal CA cert	Strong cipher suites
Database connections	TLS 1.2+	DB-specific cert	Enforce SSL
API calls	HTTPS/TLS 1.3	API Gateway cert	No HTTP allowed
VPN	IPsec or WireGuard	Mutual TLS	AES-256-GCM
SSH	SSH-2	Ed25519 keys	No password auth

Prohibited Algorithms: - DES, 3DES, RC4 - MD5, SHA-1 (except non-cryptographic use) - RSA < 2048 bits - SSL, TLS 1.0, TLS 1.1

Encryption Procedures: See Encryption Procedures

3.5 Incident Response Policy

Policy Statement: All security incidents must be promptly detected, reported, contained, and resolved using a structured incident response process to minimize business impact and ensure regulatory compliance.

Incident Definition: An event that compromises or has the potential to compromise the confidentiality, integrity, or availability of information systems or data.

Incident Categories:

Category	Examples	Response Time	Escalation
P1 - Critical	Data breach, ransomware, complete service outage	15 minutes	CISO, CEO immediate
P2 - High	Malware outbreak, DDoS, privilege escalation	1 hour	CISO, CIO within 4 hours

Category	Examples	Response Time	Escalation
P3 - Medium	Phishing campaign, policy violation, vulnerability	4 hours	Security Manager
P4 - Low	Failed login attempts, spam, minor policy breach	24 hours	Security Team

Incident Response Phases:

1. Preparation: - 24/7 SOC staffing - Incident response playbooks - Communication templates - Forensics tools pre-deployed - Regular tabletop exercises (quarterly)

2. Detection & Analysis: - Automated alerting via SIEM - Security event correlation - Threat intelligence integration - Initial triage and classification - Incident commander assignment

3. Containment, Eradication & Recovery: - Short-term containment (isolate affected systems) - Long-term containment (patch vulnerabilities) - Eradication (remove malware, close backdoors) - Recovery (restore from backups, verify integrity) - Monitoring for re-infection

4. Post-Incident Activity: - Incident report within 48 hours - Lessons learned meeting - Playbook updates - Root cause analysis - Metrics and KPIs update

Incident Communication:

Internal Communication: - Incident commander → CISO (immediate for P1/P2) - CISO → CEO (P1 within 1 hour, P2 within 4 hours) - Security team → Affected departments (ASAP) - Legal team (for potential breach notification)

External Communication: - Customers: If data breach affects them (per GDPR < 72 hours) - Regulators: As required by law (GDPR, HIPAA) - Law enforcement: For criminal activity - Media: Only via approved spokesperson - Cyber insurance: Within 24 hours of P1 incident

Breach Notification: - **GDPR:** < 72 hours to supervisory authority - **HIPAA:** < 60 days, or < 60 days end of year for < 500 affected - **CCPA:** Without unreasonable delay - **State laws:** Varies by state (e.g., California < 60 days)

Incident Response Procedures: See Incident Handling Procedures

3.6 Acceptable Use Policy (AUP)

Policy Statement: All users of organizational information systems must use resources responsibly, securely, and in compliance with legal and regulatory requirements.

Acceptable Use: - Business-related activities - Approved personal use (email, web browsing during breaks) - Learning and professional development - Authorized testing and development

Prohibited Activities: - Installing unauthorized software - Accessing inappropriate content (illegal, offensive) - Sharing credentials or allowing unauthorized access - Bypassing security controls - Using personal cloud storage for business data - Cryptocurrency mining on company resources -

Connecting unauthorized devices to network - Violating software licenses - Harassment or discrimination via IT systems

Monitoring & Enforcement: - Email and internet usage monitored for security - No expectation of privacy on company systems - Violations investigated by security team - Disciplinary action per HR policy (warning → suspension → termination)

BYOD (Bring Your Own Device): - Only if enrolled in Mobile Device Management (MDM) - Encryption required - Remote wipe capability - Security updates mandatory - No access to critical systems from BYOD

Acceptable Use Procedures: See Acceptable Use Procedures

3.7 Change Management Policy

Policy Statement: All changes to production systems must follow a documented, approved change management process to minimize risk and ensure business continuity.

Change Types:

Change Type	Approval Required	Testing	Rollback Plan
Emergency	CISO or delegate	Best effort	Mandatory
Standard	Change Advisory Board (CAB)	Required	Mandatory
Pre-approved	Auto-approved template	Required	Mandatory
Low-risk	Automated approval	Automated tests	Automated

Change Process: 1. Change request submitted via ticketing system 2. Risk assessment by security team 3. CAB review and approval (or auto-approval) 4. Implementation in maintenance window 5. Post-implementation review 6. Documentation update

Deployment Windows: - **Production:** Tuesdays/Thursdays 10 PM - 2 AM (low traffic) - **Emergency:** Any time with CISO approval - **Development:** Any time - **Staging:** Any time

Change Management Procedures: See Change Management Procedures

---

4. Governance Structure

4.1 Organizational Chart

```
Board of Directors
    ↓
Risk & Audit Committee (Oversight)
    ↓
Chief Executive Officer (CEO)
    ↓
Chief Information Security Officer (CISO)
       Cloud Security Engineering Team
          Cloud Security Architect (Lead)
          AWS Security Specialist
```

```
        Azure Security Specialist
        Security Automation Engineer
        DevSecOps Engineers (2)

    Security Operations Center (SOC)
        SOC Manager
        SOC Analysts - Tier 1 (3, 24/7 coverage)
        SOC Analysts - Tier 2 (2)
        Threat Intelligence Analyst
        Incident Response Lead

    Governance, Risk & Compliance (GRC)
        Compliance Officer (Lead)
        Compliance Analysts (2)
        Privacy Officer
        Risk Analyst

    Identity & Access Management (IAM)
        IAM Administrator
        Privileged Access Manager

    Security Engineering & Research
        Application Security Engineer
        Network Security Engineer
        Security Researcher
```

4.2 Roles & Responsibilities

4.2.1 Chief Information Security Officer (CISO)

Reports To: CEO
Direct Reports: 4-5 security leaders

Responsibilities: - Strategic security vision and roadmap - Security budget management ($2.5M+ annually) - Board and executive reporting (monthly) - Regulatory relationships and compliance strategy - Crisis management and incident escalation - Security culture and awareness programs - Third-party risk oversight - Merger & acquisition security due diligence

Key Metrics: - Security incidents (trend down) - Compliance audit results (> 98% pass rate) - Security KPIs (MTTD, MTTR, vuln remediation) - Training completion rate (100% target) - Budget variance (< 5%)

Required Skills: - 10+ years security experience, 5+ in leadership - CISSP, CISM, or equivalent certification - Cloud security expertise (AWS, Azure) - Regulatory compliance knowledge (GDPR, HIPAA) - Business acumen and communication skills

4.2.2 Cloud Security Engineer (Lead)

Reports To: CISO
Direct Reports: 5-6 engineers

Responsibilities: - Cloud security architecture design - Security control implementation (IAM, encryption, monitoring) - Infrastructure as Code security (Terraform, CloudFormation) - Security automation and orchestration - Cloud security tool selection and management - Security best practices and standards - Technical mentorship of security team

Key Metrics: - Cloud misconfiguration incidents (trend down) - CSPM compliance score (> 95%) - Security automation coverage (> 80%) - IaC security scan pass rate (> 98%) - Critical vulnerability remediation time (< 24 hours)

Required Skills: - 5+ years cloud security experience - AWS/Azure/GCP certifications (Security Specialty) - IaC expertise (Terraform, CloudFormation) - Scripting/automation (Python, Bash) - Security tools (CSPM, SIEM, SOAR)

4.2.3 Compliance Officer **Reports To:** CISO
Direct Reports: 3-4 compliance staff

Responsibilities: - Regulatory compliance strategy (GDPR, HIPAA, CCPA) - Compliance risk assessments - Audit coordination (internal and external) - Policy development and maintenance - Compliance training programs - Regulatory reporting and filings - Data protection impact assessments (DPIA) - Privacy program management

Key Metrics: - Compliance audit pass rate (> 98%) - Regulatory fines ($0 target) - Policy review completion (100% annually) - Training completion rate (100%) - DPIA completion (100% for new projects)

Required Skills: - 5+ years compliance experience - CIPP, CIPM, or equivalent certification - GDPR, HIPAA, CCPA expertise - Audit and assessment methodology - Legal and regulatory knowledge

4.2.4 Security Operations Manager (SOC Manager) **Reports To:** CISO
Direct Reports: 10-12 SOC staff

Responsibilities: - 24/7 SOC operations management - Incident detection and response - SIEM management and tuning - Threat intelligence program - Security event correlation and analysis - Incident metrics and reporting - Shift scheduling and training - Playbook development and maintenance

Key Metrics: - MTTD (< 15 minutes) - MTTR (< 1 hour for P1, < 4 hours for P2) - False positive rate (< 10%) - SOC staff utilization (70-80%) - Incident escalation accuracy (> 95%)

Required Skills: - 7+ years security operations experience - SIEM expertise (Splunk, Sentinel) - Incident response and forensics - Threat intelligence and hunting - Team management and leadership

4.2.5 Risk Management Committee **Members:** - CISO (Chair) - CIO - CFO - Chief Legal Officer - Business unit heads

Responsibilities: - Risk appetite definition - Risk acceptance decisions (for high/critical risks) - Security investment prioritization - Strategic security initiatives approval - Quarterly risk posture reviews

Meetings: Quarterly + ad-hoc for major incidents

4.3 Governance Committees

4.3.1 Change Advisory Board (CAB) **Purpose:** Approve changes to production systems

Members: - Cloud Security Engineer (Chair) - Infrastructure Lead - Application Development Lead - Database Administrator - Business stakeholder (as needed)

Meetings: Weekly + emergency meetings as needed

Responsibilities: - Review and approve change requests - Assess change risk and impact - Schedule change windows - Post-implementation review

4.3.2 Security Architecture Review Board (SARB) **Purpose:** Review security architecture for new projects

Members: - Cloud Security Architect (Chair) - Application Security Engineer - Network Security Engineer - Compliance Officer

Meetings: Bi-weekly + project-specific reviews

Responsibilities: - Security design review for new applications - Threat modeling workshops - Security standard exception approvals - Technology evaluation from security perspective

4.3.3 Incident Review Board **Purpose:** Post-incident analysis and continuous improvement

Members: - CISO (Chair) - SOC Manager - Incident Response Lead - Affected business unit representative - Compliance Officer (for breach incidents)

Meetings: Within 48 hours of P1/P2 incident resolution

Responsibilities: - Root cause analysis - Lessons learned identification - Corrective action planning - Playbook updates - Communication plan review

4.4 Oversight & Monitoring Mechanisms

4.4.1 Continuous Monitoring **Real-Time Monitoring:** - SIEM alert monitoring (24/7 SOC) - Cloud security posture (CSPM scans every hour) - Vulnerability scanning (daily) - Threat intelligence feeds (real-time) - User behavior analytics (UEBA)

Dashboards: - Executive dashboard (weekly review) - Security operations dashboard (real-time) - Compliance dashboard (daily review) - Risk heat map (monthly review)

Automation: - Automated incident creation in SIEM - Automated remediation for common issues - Automated compliance checks - Automated reporting

4.4.2 Audit & Assessment Schedule

Activity	Frequency	Owner	Audience
Internal security audit	Quarterly	Compliance team	CISO, Risk Committee
External SOC 2 audit	Annually	External auditor	Customers, board
Penetration testing	Quarterly	External firm	CISO, Cloud Security Engineer
Vulnerability assessment	Weekly	Security team	Security operations

Activity	Frequency	Owner	Audience
Compliance assessment	Monthly	Compliance Officer	CISO, regulators
Risk assessment	Quarterly	Risk analyst	Risk Committee
Security awareness campaign	Monthly	Compliance Officer	All employees
Disaster recovery test	Bi-annually	SOC Manager	CISO, business continuity
Vendor security review	Annually	Vendor risk manager	CISO, procurement
Access review	Quarterly	IAM team	Department managers

4.4.3 Reporting Structure **Daily Reports:** - Security incident summary (SOC → CISO) - Critical vulnerability summary (Security team → Cloud Security Engineer)

Weekly Reports: - Security metrics (CISO → Executive team) - Change summary (CAB → CISO)

Monthly Reports: - Compliance status (Compliance Officer → CISO → Board Risk Committee) - Security KPIs (CISO → CEO) - Vendor risk summary (Vendor risk manager → CISO)

Quarterly Reports: - Risk posture (CISO → Risk Committee → Board) - Security program maturity (CISO → Board) - Training and awareness (Compliance Officer → CISO)

Annual Reports: - Comprehensive security assessment (CISO → Board) - Compliance certifications (SOC 2, ISO 27001) - Security strategy and roadmap (CISO → Board)

4.5 Budget & Resource Allocation

Year 1 Security Budget: $2,450,000

Budget Breakdown:

Category	Amount	%	Justification
Personnel	$650,000	27%	15 FTEs (mix of existing + new hires)
Security Tools	$850,000	35%	SIEM, CSPM, EDR, PAM, etc.
Cloud Security Services	$400,000	16%	GuardDuty, Security Hub, Shield
Professional Services	$250,000	10%	Pen testing, audit, consulting
Training & Certifications	$150,000	6%	Team development, conferences
Compliance & Audit	$100,000	4%	External audits, legal
Incident Response	$50,000	2%	Forensics, crisis management
Total	**$2,450,000**	**100%**	

Tool Budget Detail:

Tool	Vendor	Annual Cost	Users
SIEM (Splunk Enterprise Security)	Splunk	$180,000	500 GB/day
CSPM (Prisma Cloud)	Palo Alto	$120,000	Multi-cloud
EDR (CrowdStrike Falcon)	CrowdStrike	$100,000	1,000 endpoints
PAM (CyberArk)	CyberArk	$90,000	50 privileged users
IAM (Okta)	Okta	$75,000	1,500 users
Vulnerability Scanning (Tenable.io)	Tenable	$60,000	Unlimited scans
DLP (Microsoft Purview)	Microsoft	$50,000	1,500 users
Email Security (Proofpoint)	Proofpoint	$40,000	1,500 mailboxes
AWS Security (GuardDuty, Security Hub)	AWS	$85,000	Multi-account
Azure Security (Sentinel, Defender)	Microsoft	$50,000	Azure estate
Total Tools		**$850,000**	

---

5. Compliance & Legal Considerations

(Continued in next response due to length…)

5.1 Regulatory Landscape

5.1.1 GDPR (General Data Protection Regulation) **Scope:** EU resident data processing

Key Requirements: - Lawful basis for processing (consent, contract, legal obligation, etc.) - Data minimization and purpose limitation - Data subject rights (access, erasure, portability, etc.) - Data protection by design and by default - Breach notification < 72 hours - Data Protection Impact Assessments (DPIA) for high-risk processing - Data Processing Agreements (DPA) with processors - Appointing a Data Protection Officer (DPO) if required

Penalties: Up to €20 million or 4% of annual global turnover, whichever is greater

Compliance Implementation: See GDPR Compliance Guide

5.1.2 HIPAA (Health Insurance Portability and Accountability Act) **Scope:** Protected Health Information (PHI)

Key Requirements: - **Privacy Rule:** Limits on PHI use and disclosure - **Security Rule:** Administrative, physical, technical safeguards - **Breach Notification Rule:** Notification requirements - **Business Associate Agreement (BAA):** Required with cloud providers

Penalties: Up to $1.5 million per violation category per year

Compliance Implementation: See HIPAA Compliance Guide

5.1.3 CCPA (California Consumer Privacy Act)

Scope: California resident data

Key Requirements: - Consumer rights (know, delete, opt-out of sale) - Privacy notice requirements - No discrimination for privacy rights exercise - Reasonable security measures

Penalties: Up to $7,500 per intentional violation, $2,500 per unintentional

Compliance Implementation: See CCPA Compliance Guide

5.2 Compliance Program

Privacy by Design: - Security and privacy integrated into system design - Default to most privacy-protective settings - DPIA for new projects handling sensitive data

Data Inventory: - Complete inventory of personal data - Data flow mapping - Regular inventory updates

Consent Management: - Granular consent options - Easy withdrawal mechanism - Audit trail of consent

Data Subject Rights: - Automated request portal - 30-day response SLA - Verification of requestor identity

Audit Schedule: - Internal compliance audits: Quarterly - External SOC 2 Type II: Annually - HIPAA assessment: Annually - GDPR audit: Annually

Compliance Automation: See Audit & Compliance Procedures

---

6. Security Tools & Technologies

(Detailed in separate sections - overview provided)

6.1 Identity & Access Management (IAM)

- Multi-factor authentication
- Single sign-on
- Privileged access management
- Identity governance

6.2 Data Protection & Encryption

- Cloud-native encryption (KMS, Key Vault)
- Data loss prevention
- Tokenization and masking

6.3 Network Security

- Web application firewall
- DDoS protection
- Network segmentation
- VPN and private connectivity

6.4 Threat Detection & Response

- SIEM and log management
- Cloud security posture management
- Endpoint detection and response
- Threat intelligence

6.5 Vulnerability Management

- Vulnerability scanning
- Penetration testing
- Patch management
- Security testing in CI/CD

6.6 Security Automation

- Infrastructure as Code security
- Security orchestration and response (SOAR)
- Automated remediation

---

7. Incident Response & Business Continuity

7.1 Incident Response Plan

24/7 SOC Operations: - Tier 1 analysts: Initial triage - Tier 2 analysts: Investigation and containment - Incident response lead: Complex incidents, coordination

Incident Response Playbooks: - Data breach response - Ransomware response - DDoS attack response - Insider threat response - Cloud compromise response - Supply chain attack response

Incident Response Procedures: See Incident Handling Procedures

7.2 Business Continuity & Disaster Recovery

RTO/RPO Targets: - Critical systems: RTO < 4 hours, RPO < 1 hour - Important systems: RTO < 24 hours, RPO < 4 hours - Normal systems: RTO < 72 hours, RPO < 24 hours

DR Strategy: - Multi-region deployment for critical workloads - Automated failover - Regular DR testing (bi-annually) - Annual tabletop exercises

Backup Strategy: - Daily incremental backups - Weekly full backups - 30-day retention (longer for compliance) - Encrypted backups with separate keys - Offsite backup storage

---

8. Implementation Plan

8.1 Phased Approach

Phase 1: Foundation (Weeks 1-4) - Risk assessment completion - Governance structure establishment - Tool procurement - Policy development

Phase 2: Design (Weeks 5-10) - Security architecture design - Detailed procedures creation - Training material development - Compliance mapping

Phase 3: Implementation (Weeks 11-22) - Security tool deployment - Team training - Policy rollout - Monitoring configuration

Phase 4: Validation (Weeks 23-26) - Security testing - Compliance audits - Penetration testing - Remediation

Phase 5: Operations (Week 27+) - 24/7 SOC operations - Continuous monitoring - Regular assessments - Continuous improvement

8.2 Success Metrics

Refer to Executive Summary for detailed KPIs

---

9. Appendices

Appendix A: Glossary

Appendix B: References

Appendix C: Document History

Appendix D: Contact Information

End of Report

Document Control: - Version: 1.0 - Classification: Confidential - Review Date: February 28, 2026 - Approval: CISO, CEO, Board Risk Committee