Cloud Security Governance Framework

Executive Presentation

CLOUD SECURITY GOVERNANCE FRAMEWORK

Securing Our Cloud Journey

Medium Enterprise Cloud Security Strategy

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

---

Executive Summary

The Challenge

We are migrating to the cloud while handling: - 100K+ customers with sensitive data - Protected Health Information (PHI) - Personally Identifiable Information (PII) - Financial records and payment data

Subject to regulations: - GDPR (€20M or 4% revenue penalties) - HIPAA ($1.5M per violation) - CCPA ($7,500 per violation)

Our Solution

Comprehensive security governance framework that: Protects sensitive data across multi-cloud (AWS, Azure, GCP)
Ensures continuous regulatory compliance
Enables secure cloud adoption without hindering innovation
Provides 24/7 threat detection and response

The Business Case

Why We Need This Framework

Risk	Cost if Realized	Likelihood	Framework Mitigation
Data Breach	$4.45M average (IBM 2023)	Medium-High	Encryption, DLP, monitoring
Regulatory Fine	Up to $20M+	Medium	Compliance automation, audits
Ransomware	$2M+ (ransom + downtime)	Medium	EDR, backups, segmentation

Risk	Cost if Realized	Likelihood	Framework Mitigation
Cloud Misconfiguration	Public data exposure	High	CSPM, IaC security
Reputational Damage	Immeasurable	High	All controls combined

Total Potential Exposure: $30M+

Our Investment

Year 1 Budget: $2.45M

ROI: Prevent one major breach = 18:1 return on investment

Framework Overview

Six Pillars of Cloud Security Governance

```
1. RISK           2. POLICIES       3. GOVERNANCE
ASSESSMENT        & PROCEDURES      STRUCTURE

4. COMPLIANCE     5. SECURITY       6. INCIDENT
& LEGAL           TOOLS/TECH        RESPONSE & DR
```

Each pillar is: - Fully documented - Measured with KPIs - Continuously monitored - Regularly reviewed

---

Pillar 1 - Risk Assessment

Comprehensive Threat Landscape

Technical Risks Identified: - **Cloud Misconfigurations** (45/75 risk score) - Open S3 buckets, overly permissive IAM - Mitigation: CSPM tools, automated scanning

- **Data Encryption Gaps** (42/75)
  - Unencrypted sensitive data
  - Mitigation: AWS KMS, Azure Key Vault, mandatory encryption
- **API Vulnerabilities** (38/75)
  - Authentication bypass, data leakage
  - Mitigation: API Gateway, rate limiting, security testing

Human Factor Risks: - **Insider Threats** (48/75) - Malicious or negligent insiders - Mitigation: UEBA, DLP, access monitoring

- **Phishing & Social Engineering** (40/75)
  - Email attacks targeting employees
  - Mitigation: Email security, MFA, security training

Third-Party Risks: - **Vendor Security Gaps** (35/75) - Compromised cloud providers or SaaS - Mitigation: Vendor assessments, SOC 2 requirements

Risk Mitigation Strategy

150+ Risks Identified → Prioritized by Impact × Likelihood

Pillar 2 - Security Policies

Zero Trust Architecture

Core Principle: "Never Trust, Always Verify"

Key Policies Implemented:

1. **Data Protection Policy**
   - Data classification (Critical, Confidential, Internal, Public)
   - AES-256 encryption mandatory for sensitive data
   - 7-year retention for PHI and financial records
2. **Access Control Policy**
   - Least privilege access (RBAC)
   - Multi-factor authentication (100% enforcement)
   - Just-in-Time (JIT) access for privileged operations
   - Quarterly access reviews
3. **Encryption Policy**
   - TLS 1.3 for data in transit
   - AES-256 for data at rest
   - Customer-managed keys (CMK) for critical data
   - 90-day key rotation
4. **Incident Response Policy**
   - < 15 minute detection (MTTD)
   - < 1 hour response (MTTR) for P1 incidents
   - 24/7 Security Operations Center
   - < 72 hour GDPR breach notification

Policy Enforcement

- Automated compliance checks (daily)
- Security training (100% annual completion)
- Regular audits (quarterly)

Pillar 3 - Governance Structure

Leadership & Oversight

```
Board of Directors
    ↓
Risk & Audit Committee (Quarterly Oversight)
    ↓
CISO
      Cloud Security Engineer (Technical Lead)
      Compliance Officer (Regulatory Lead)
      SOC Manager (24/7 Operations)
      Risk Management Committee (Strategic Decisions)
```

Team Size: 15 FTEs (Year 1)

Key Roles: - **CISO:** Strategic vision, budget, board reporting - **Cloud Security Engineer:** AWS/Azure security architecture - **Compliance Officer:** GDPR, HIPAA, CCPA compliance - **SOC Team:** 24/7 monitoring, incident response

Governance Committees

Committee	Purpose	Frequency
Risk Management Committee	Risk appetite, investment decisions	Quarterly
Change Advisory Board (CAB)	Approve production changes	Weekly
Security Architecture Review Board	New project security reviews	Bi-weekly
Incident Review Board	Post-incident analysis	After P1/P2 incidents

---

Pillar 4 - Compliance & Legal

Regulatory Compliance

GDPR (General Data Protection Regulation) - Scope: EU customer data - **Key Requirements:** - Data protection by design - < 72 hour breach notification - Data subject rights (access, erasure, portability) - Data Protection Impact Assessments (DPIA) - **Penalty:** Up to €20M or 4% revenue - **Our Approach:** Privacy Officer, DPA with cloud providers, automated consent management

HIPAA (Health Insurance Portability and Accountability Act) - Scope: Protected Health Information (PHI) - **Key Requirements:** - Administrative, physical, technical safeguards - Business Associate Agreements (BAA) - Access logging and encryption - Breach notification - **Penalty:** Up to $1.5M per violation - **Our Approach:** BAA with AWS/Azure, PHI encryption, audit logging

CCPA (California Consumer Privacy Act) - Scope: California resident data - **Key Requirements:** - Consumer rights (know, delete, opt-out) - Privacy notices - Reasonable security -

Penalty: Up to $7,500 per violation - **Our Approach:** Data inventory, consent portal, privacy notices

Compliance Program

Quarterly internal compliance audits
Annual external SOC 2 Type II audit
Automated compliance monitoring (95%+ score target)
Regular regulatory training (100% completion)
Legal counsel for breach notification

Pillar 5 - Security Tools & Technologies

Technology Stack

Identity & Access Management - Multi-Factor Authentication (Okta, Duo) - Single Sign-On across all cloud platforms - Privileged Access Management (CyberArk) - Just-in-Time access provisioning

Data Protection & Encryption - AWS KMS, Azure Key Vault, Google Cloud KMS - Data Loss Prevention (Microsoft Purview, Symantec) - Tokenization for payment data - Field-level encryption in applications

Network Security - Web Application Firewall (AWS WAF, Azure Firewall) - DDoS Protection (AWS Shield Advanced, Azure DDoS) - Network segmentation (VPC, subnets, security groups) - VPN and Private Link for secure connectivity

Threat Detection & Response - SIEM: Splunk Enterprise Security ($180K/year) - Cloud Security Posture Management: Prisma Cloud ($120K/year) - Endpoint Detection & Response: CrowdStrike Falcon ($100K/year) - Cloud-native: AWS GuardDuty, Azure Sentinel, Google SCC - User Behavior Analytics (UEBA) for insider threat detection

Vulnerability Management - Automated scanning: AWS Inspector, Azure Defender, Tenable.io - Penetration testing: Quarterly by external firms - Secure CI/CD: Snyk, Aqua Security for container scanning - Bug bounty program for responsible disclosure

Security Automation

- Infrastructure as Code security (Terraform, CloudFormation)
- Automated remediation (AWS Lambda, Azure Functions)
- Security Orchestration (SOAR) for incident response
- CI/CD security gates (block on critical vulnerabilities)

Pillar 6 - Incident Response & Business Continuity

Incident Response Program

24/7 Security Operations Center (SOC)

```
Incident Detection (SIEM, CSPM, EDR)
    ↓
Tier 1 Analyst: Triage (< 15 minutes MTTD)
    ↓
Tier 2 Analyst: Investigation & Containment (< 1 hour MTTR)
    ↓
Incident Response Lead: Coordination & Executive Comms
    ↓
Post-Incident Review (< 48 hours)
    ↓
Lessons Learned & Continuous Improvement
```

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

Business Continuity & Disaster Recovery

RTO/RPO Targets: - **Critical Systems:** RTO < 4 hours, RPO < 1 hour - **Important Systems:** RTO < 24 hours, RPO < 4 hours

DR Strategy: - Multi-region deployment (AWS: us-east-1, us-west-2) - Automated failover for critical workloads - Daily incremental backups, weekly full backups - 30-day backup retention (extended for compliance) - Bi-annual disaster recovery testing - Annual tabletop exercises

Breach Notification

Regulatory Timelines: - GDPR: < 72 hours to supervisory authority - HIPAA: < 60 days (or end of year for small breaches) - CCPA: Without unreasonable delay

Our Readiness: - Pre-drafted notification templates - Legal team on retainer - Cyber insurance ($10M coverage) - Crisis communication plan

---

Implementation Roadmap

Phased Approach (26 Weeks)

Phase 1: Foundation (Weeks 1-4) - Complete comprehensive risk assessment - Establish governance structure and committees - Finalize security baseline and architecture - Procure security tools and cloud services

Phase 2: Design & Planning (Weeks 5-10) - Develop detailed policies and procedures - Design multi-cloud security architecture - Create compliance mapping (GDPR, HIPAA, CCPA) - Build incident response playbooks - Develop training materials

Phase 3: Deployment (Weeks 11-22) - Deploy security tools (SIEM, CSPM, EDR, PAM) - Configure monitoring and alerting - Implement access controls and encryption - Train security team (certifications, tools) - Roll out employee security awareness program

Phase 4: Validation (Weeks 23-26) - Security testing (vulnerability scans, pen testing) - Compliance audits (internal + external SOC 2) - Tabletop incident response exercises - Remediation and tuning - Executive readiness review

Phase 5: Operations (Week 27+) - 24/7 SOC operations begin - Continuous monitoring and improvement - Regular compliance assessments - Quarterly risk reviews - Annual framework updates

---

Budget & Resources

Year 1 Investment: $2.45 Million

Category	Amount	% of Budget
Security Tools & Licenses	$850,000	35%
Personnel & Training	$650,000	27%
Professional Services	$400,000	16%
Compliance & Audits	$250,000	10%
Incident Response & DR	$200,000	8%
Insurance & Legal	$100,000	4%

Staffing Plan

Year 1 Team (15 FTEs): - 1x CISO (Senior Leadership) - 2x Cloud Security Engineers (AWS, Azure specialists) - 1x Compliance Officer - 6x SOC Analysts (24/7 coverage) - 2x DevSecOps Engineers - 2x Compliance Analysts - 1x Incident Response Lead

Year 2-3: +5-7 FTEs as cloud adoption scales

Key Tool Investments

- **SIEM** (Splunk): $180K
- **CSPM** (Prisma Cloud): $120K
- **EDR** (CrowdStrike): $100K
- **PAM** (CyberArk): $90K
- **IAM** (Okta): $75K
- **Cloud Security** (GuardDuty, Sentinel): $135K

Success Metrics & KPIs

Security Metrics

Metric	Current State	Target	Timeline
Mean Time to Detect (MTTD)	Unknown	< 15 min	6 months
Mean Time to Respond (MTTR)	Unknown	< 1 hour	6 months
Critical Vuln Remediation	~7 days	< 24 hours	3 months
Phishing Click Rate	12%	< 5%	12 months
MFA Adoption	30%	100%	3 months
Security Training Completion	65%	100%	6 months
CSPM Compliance Score	75%	> 95%	6 months

Compliance Metrics

Metric	Target
Compliance Audit Pass Rate	> 98%
Regulatory Fines	$0
Policy Violations	< 5 per quarter
Data Breach Incidents	0
SOC 2 Certification	Achieved by Month 12

Business Impact Metrics

Metric	Expected Outcome
Cloud Migration Delay	0 days (security enables migration)
Security Incidents (P1/P2)	< 5 per quarter
Customer Trust Score	Increase (security certification)
Cyber Insurance Premium	Decrease 15% (better posture)
Competitive Advantage	Security as differentiator

Risk Mitigation Summary

Before Framework (Current State)

No dedicated security team - IT staff juggling security
No SIEM or centralized monitoring - Security blind spots
No cloud security tools - Misconfigurations undetected
Inconsistent MFA - 30% adoption, password risks
Manual compliance - Labor-intensive, error-prone
No 24/7 monitoring - After-hours incidents go undetected
No incident response plan - Reactive, chaotic response
Regulatory non-compliance - Potential fines, audit failures

Risk Level: HIGH

After Framework (Future State)

15-person security team - Dedicated expertise
24/7 SOC with SIEM - Real-time threat detection
Cloud-native security tools - Proactive misconfiguration prevention
100% MFA enforcement - Strong authentication
Automated compliance monitoring - Continuous, accurate
Round-the-clock coverage - No security gaps
Comprehensive IR playbooks - Structured, tested response
Regulatory compliance - GDPR, HIPAA, CCPA ready

Risk Level: LOW

Competitive Advantage

How Security Enables Business

Customer Trust: - Security certifications (SOC 2, ISO 27001) as competitive differentiator - Transparent security posture for enterprise customers - Regulatory compliance as table stakes for healthcare/finance deals

Faster Time-to-Market: - Secure cloud adoption without delays - DevSecOps integration for rapid, secure deployments - Automated security gates in CI/CD

Cost Savings: - Prevent breach costs ($4.45M average) - Avoid regulatory fines ($20M+ potential) - Reduce cyber insurance premiums (15% estimated savings) - Cloud cost optimization through right-sized security

Business Enablement: - Secure expansion into new markets (EU with GDPR compliance) - Mergers & acquisitions (due diligence readiness) - Partner integrations (secure API ecosystem)

Recommendations

Immediate Actions (Next 30 Days)

1. **Approve $2.45M Year 1 Budget**
   - Critical for framework deployment
   - ROI: Prevent one major breach = 18:1 return
2. **Appoint CISO**
   - Begin executive search if position not filled
   - Target: Hire within 60 days
3. **Initiate Risk Assessment**
   - Engage third-party for comprehensive review
   - Timeline: 4 weeks
4. **Cloud Deployment Pause (Optional)**
   - Halt non-essential cloud deployments until security controls in place
   - Alternative: Accelerated deployment with risk acceptance
5. **Legal Review**
   - Engage counsel for DPAs, BAAs, compliance strategy
   - Timeline: 2 weeks

Strategic Priorities (Next 90 Days)

1. **Build Security Team** - Hire 10+ security professionals
2. **Deploy Core Tools** - IAM, encryption, SIEM, CSPM
3. **Establish Governance** - Charter committees, define processes
4. **Compliance Baseline** - Gap analysis for GDPR, HIPAA, CCPA
5. **Launch Training** - Security awareness program for all employees

---

Conclusion

Why This Framework Matters

The Stakes: - **Data Breach:** $4.45M average cost + reputational damage - **Regulatory Fines:** Up to $20M+ for GDPR violations - **Business Disruption:** Days/weeks to recover from ransomware - **Customer Trust:** Lost business from security incidents

Our Framework Delivers: - **Comprehensive Protection:** Defense-in-depth across all layers - **Regulatory Compliance:** GDPR, HIPAA, CCPA ready - **24/7 Monitoring:** Proactive threat detection and response - **Business Enablement:** Secure cloud adoption without delays - **Proven ROI:** Prevent one breach = 18:1 return on investment

The Path Forward

Investment: $2.45M (Year 1)
Timeline: 26 weeks to full deployment
Team: 15 dedicated security professionals
Outcome: Enterprise-grade cloud security governance

Call to Action

Board Approval Requested: 1. Approve $2.45M Year 1 security budget 2. Authorize CISO hire (if not filled) 3. Endorse framework implementation timeline 4. Support quarterly risk posture reviews

Expected Board Vote: [Date]

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

Supporting Documents: - Executive Summary - Comprehensive Framework Report (100+ pages) - Governance Structure Diagrams - Security Policies & Procedures - Compliance Guides (GDPR, HIPAA, CCPA)

Appendix: Additional Slides

Appendix A: Risk Heat Map

```
IMPACT →
    HIGH     M     H    C    C

    MED      L     M    M    H

    LOW      L     L    M    M

            LOW  MED  HIGH CRIT
                ← LIKELIHOOD
```

```
Legend:
L = Low Risk (1-9)
M = Medium Risk (10-24)
H = High Risk (25-49)
C = Critical Risk (50-75)
```

Top Risks: - Insider threat (48) - Critical - Cloud misconfiguration (45) - High - Encryption gaps (42) - High - Phishing attacks (40) - High

---

Appendix B: Cloud Security Architecture

```
          INTERNET / USERS

              ↓

  WAF + DDoS Protection
  (AWS Shield, Azure DDoS)

              ↓

  Application Load Balancer (Public Subnet)
  + TLS 1.3 Termination

              ↓

  Application Tier (Private Subnet)
  • Containers (ECS, AKS)
  • Encryption in transit
  • IAM roles for access

              ↓

  Database Tier (Private Subnet)
  • RDS with encryption (TDE + KMS)
  • No internet access
  • Backups encrypted


Monitoring & Security:
  CloudTrail / Azure Activity Logs (All API calls)
  VPC Flow Logs (Network traffic)
  GuardDuty / Sentinel (Threat detection)
  Security Hub / Security Center (Posture management)
  SIEM (Splunk) - Centralized logging
```

Appendix C: Compliance Mapping

GDPR Requirement	Implementation	Owner
Data protection by design	Privacy reviews in SARB	Compliance Officer
Breach notification < 72hr	IR playbook, legal team	SOC Manager
Data subject rights	Automated portal	Compliance Officer
DPIA for high-risk	Mandatory for new projects	Privacy Officer
DPA with processors	Cloud provider contracts	Legal + CISO

HIPAA Requirement	Implementation	Owner
Access controls	IAM + MFA + PAM	IAM Administrator
Audit controls	CloudTrail + SIEM logging	SOC Manager
Encryption at rest/transit	KMS + TLS 1.3	Cloud Security Engineer
BAA with cloud providers	AWS, Azure contracts	Legal + CISO
Incident response	IR playbooks, 24/7 SOC	SOC Manager

Appendix D: Vendor Security Assessment

Tier 1 Vendors (Critical): - AWS, Azure, Google Cloud - Okta (IAM) - Splunk (SIEM)

Requirements: - SOC 2 Type II (annual) - ISO 27001 certification - Right to audit clause - Dedicated account manager - < 24 hour breach notification - $10M+ cyber insurance

Assessment Process: 1. Security questionnaire (SIG Lite) 2. SOC 2 report review 3. Penetration test results 4. Reference checks 5. On-site security visit (for critical vendors) 6. Annual recertification