PACT Protocol Security Architecture & Threat Model

Comprehensive Security Assessment for Enterprise and Government Deployment

Prepared for: Chief Information Security Officers, Security Architects, Compliance Officers

Prepared by: ARKA Systems LLC Security Engineering

Document Classification: CISO Reference Document

Version: 1.0

Date: December 2024

Review Cycle: Quarterly

Executive Summary

This document presents the comprehensive security architecture and threat model for the PACT Protocol. It is designed for CISO review and maps to established frameworks including NIST 800-53, CIS Controls, and SOC 2 Type II requirements.

PACT implements a **defense-in-depth** strategy across four distinct layers:

1. **PACT Engine** - Deterministic rule execution with input validation
2. **PACT Cloud** - Multi-tenant SaaS with isolation guarantees
3. **PACT AI** - Supervised machine learning with guardrails
4. **PACT Blockchain** - Permissioned ledger with Byzantine fault tolerance

The architecture assumes a **zero-trust posture** where no component, user, or network segment is implicitly trusted.

1. Zero-Trust Architecture

1.1 Architectural Principles

PACT implements zero-trust through six core principles:

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ZERO-TRUST ARCHITECTURE ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■
■ ■ PRINCIPLE 1: VERIFY EXPLICITLY ■ ■
■ ■ ■ ■
■ ■ • Every request authenticated via mTLS or JWT ■ ■
■ ■ • User identity validated against IdP on every call ■ ■
■ ■ • Device posture assessed before access granted ■ ■
■ ■ • Context (time, location, behavior) evaluated ■ ■
■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■
■ ■
■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■
■ ■ PRINCIPLE 2: LEAST PRIVILEGE ■ ■
■ ■ ■ ■
■ ■ • Role-based access control (RBAC) with granular permissions ■ ■
■ ■ • Just-in-time (JIT) access for sensitive operations ■ ■
■ ■ • Service accounts scoped to minimum required permissions ■ ■
■ ■ • Regular access reviews and automatic deprovisioning ■ ■
■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■
■ ■
■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■
■ ■ PRINCIPLE 3: ASSUME BREACH ■ ■
■ ■ ■ ■
■ ■ • Micro-segmentation between all services ■ ■
■ ■ • East-west traffic inspection and logging ■ ■
■ ■ • Blast radius containment through isolation ■ ■
■ ■ • Continuous monitoring for lateral movement ■ ■
■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■
```

1.2 Network Architecture

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ NETWORK ZONES ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ ZONE 0: PUBLIC (Internet-Facing) ■
■ ■■■ CloudFront CDN (DDoS protection) ■
■ ■■■ AWS WAF (OWASP Top 10 rules) ■
■ ■■■ API Gateway (rate limiting, authentication) ■
■ ■ ■
■ ■ [TLS 1.3 only] ■
■ ▼ ■
■ ZONE 1: DMZ (Application Layer) ■
■ ■■■ Application Load Balancers ■
■ ■■■ API Services (stateless, containerized) ■
■ ■■■ Authentication Service ■
■ ■ ■
■ ■ [mTLS required] ■
■ ▼ ■
■ ZONE 2: APPLICATION (Business Logic) ■
■ ■■■ PACT Engine (isolated ECS tasks) ■
■ ■■■ PACT Cloud Services (microservices mesh) ■
■ ■■■ PACT AI Workers (Bedrock VPC endpoint) ■
■ ■ ■
■ ■ [Private subnets only] ■
■ ▼ ■
■ ZONE 3: DATA (Persistence Layer) ■
■ ■■■ RDS PostgreSQL (encrypted at rest) ■
■ ■■■ DynamoDB (encryption, point-in-time recovery) ■
■ ■■■ S3 (SSE-KMS, versioning, object lock) ■
■ ■ ■
```

1.3 Identity and Access Management

Component	Authentication	Authorization	MFA Required
API Gateway	JWT (Cognito/OIDC)	RBAC policies	Yes
Service-to-Service	mTLS certificates	Service mesh policies	N/A
Admin Console	SAML 2.0 SSO	Attribute-based (ABAC)	Yes (hardware key)
Validator Nodes	HSM-backed keys	Validator registry	N/A
Database Access	IAM authentication	Row-level security	N/A
AI/Bedrock	IAM roles (assumed)	Resource policies	N/A

2. Threat Vectors (RegTech-Specific)

2.1 Threat Landscape Overview

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ REGTECH THREAT LANDSCAPE ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ THREAT ACTOR CATEGORIES ■
■ ■■■ Nation-State Actors (APT) ■
■ ■ ■■■ Objective: Surveillance, sanctions evasion, economic warfare ■
■ ■■■ Organized Crime ■
■ ■ ■■■ Objective: Money laundering, fraud, compliance evasion ■
■ ■■■ Insider Threats ■
■ ■ ■■■ Objective: Data theft, rule manipulation, sabotage ■
■ ■■■ Hacktivists ■
■ ■ ■■■ Objective: Disruption, data leaks, reputation damage ■
■ ■■■ Competitors ■
■ ■■■ Objective: IP theft, customer poaching, sabotage ■
■ ■
■ REGTECH-SPECIFIC ATTACK OBJECTIVES ■
■ ■■■ Compliance Evasion: Manipulate rules to allow illicit activity ■
■ ■■■ Audit Trail Tampering: Modify or delete evidence of violations ■
■ ■■■ AI Manipulation: Poison training data or exploit model weaknesses ■
■ ■■■ Sanctions Bypass: Circumvent screening to process blocked parties ■
■ ■■■ Regulatory Arbitrage: Exploit inconsistencies across jurisdictions ■
■ ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

2.2 Detailed Threat Matrix

Threat ID	Threat Vector	Target Component	Likelihood	Impact	Risk Score
T-001	Rule Injection	PACT Engine	Medium	Critical	High
T-002	Audit Log Tampering	Cloud/Database	Medium	Critical	High
T-003	AI Model Poisoning	PACT AI	Low	High	Medium
T-004	Validator Key Compromise	Blockchain	Low	Critical	High
T-005	Attestation Fraud	AI-Blockchain Bridge	Medium	High	High
T-006	Oracle Data Manipulation	External Feeds	Medium	High	High
T-007	Privilege Escalation	IAM/Access Control	Medium	Critical	High
T-008	Data Exfiltration	All Layers	Medium	Critical	High
T-009	Denial of Service	API/Blockchain	High	Medium	Medium
T-010	Supply Chain Attack	Dependencies	Low	Critical	Medium

2.3 Attack Trees

T-001: Rule Injection Attack

```
GOAL: Execute unauthorized compliance rule

■

■■■ [OR] Compromise Rule Authoring System

■ ■■■ [AND] Phishing attack on rule author

■ ■ ■■■ Bypass MFA

■ ■■■ [AND] Compromise CI/CD pipeline
■ ■ ■■■ Inject malicious rule in PR
■ ■■■ [AND] Insider threat
■ ■■■ Collude with approver
■
■■■ [OR] Bypass Approval Workflow
■ ■■■ [AND] Exploit approval system vulnerability
■ ■■■ [AND] Social engineering of approvers
■
■■■ [OR] Direct Database Manipulation
■■■ [AND] Compromise database credentials
■ ■■■ Bypass encryption
■■■ [AND] Exploit SQL injection
■■■ Bypass input validation

MITIGATIONS:
• Multi-party approval (minimum 2 approvers)
• Cryptographic signing of rules
• Immutable rule history on blockchain
• Automated regression testing
• Anomaly detection on rule changes
```

T-004: Validator Key Compromise

```
GOAL: Control blockchain consensus
■
■■■ [OR] Physical Key Theft
■ ■■■ [AND] Access to HSM
■ ■ ■■■ Bypass physical security
■ ■■■ [AND] Insider with HSM access
■ ■■■ Export key material
■
```

```
■■■ [OR] Remote Key Extraction
■ ■■■ [AND] Exploit HSM firmware
■ ■ ■■■ Zero-day vulnerability
■ ■■■ [AND] Side-channel attack
■ ■■■ Timing/power analysis
■
■■■ [OR] Key Generation Weakness
■■■ [AND] Weak entropy source
■■■ [AND] Compromised key ceremony

MITIGATIONS:
• FIPS 140-3 Level 3 HSMs
• Multi-signature schemes (threshold)
• Key rotation every 90 days
• Geographically distributed key shares
• Ceremony with multiple witnesses
```

3. Access Control Enforcement & Encryption

3.1 Access Control Architecture

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ACCESS CONTROL LAYERS ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ LAYER 1: PERIMETER (Network) ■
■ ■■■ AWS Security Groups (stateful firewall) ■
■ ■■■ Network ACLs (stateless firewall) ■
■ ■■■ VPC Flow Logs (traffic analysis) ■
■ ■■■ AWS Shield Advanced (DDoS protection) ■
■ ■
■ LAYER 2: APPLICATION (API) ■
■ ■■■ API Gateway authorization (JWT validation) ■
■ ■■■ Rate limiting (per-user, per-tenant) ■
■ ■■■ Request signing (HMAC-SHA256) ■
■ ■■■ Input validation (schema enforcement) ■
■ ■
■ LAYER 3: SERVICE (Business Logic) ■
■ ■■■ Service mesh policies (Istio/App Mesh) ■
■ ■■■ RBAC enforcement (permission checks) ■
■ ■■■ Tenant isolation (data partitioning) ■
■ ■■■ Audit logging (all access recorded) ■
■ ■
■ LAYER 4: DATA (Persistence) ■
■ ■■■ Row-level security (PostgreSQL RLS) ■
■ ■■■ Attribute-based encryption (field-level) ■
■ ■■■ IAM database authentication ■
■ ■■■ Query logging and analysis ■
■ ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

3.2 Role-Based Access Control Matrix

Role	Rules	Transactions	AI Analysis	Attestations	Admin
System Admin	R	R	R	R	CRUD
Compliance Officer	RU	R	R	R	R

Rule Author	CRU	R	R	R	-
Rule Approver	RU	R	R	R	-
Analyst	R	R	R	R	-
Auditor	R	R	R	R	R
Regulator	R	R	R	R	R
API Client	-	CR	R	R	-

C=Create, R=Read, U=Update, D=Delete

3.3 Encryption Architecture

3.3.1 Key Hierarchy

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ KEY HIERARCHY ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■
■ ■ ROOT KEY (AWS KMS) ■ ■
■ ■ CMK stored in FIPS 140-2 Level 3 HSM ■ ■
■ ■ Automatic annual rotation ■ ■
■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■
■ ■ ■
■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■
■ ▼ ▼ ▼ ■
■ ■■■■■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■■■ ■
■ ■ DATA KEYS ■ ■ SERVICE KEYS ■ ■ BLOCKCHAIN KEYS ■ ■
■ ■ ■ ■ ■ ■ ■ ■
■ ■ • Database DEKs ■ ■ • API signing ■ ■ • Validator ■ ■
■ ■ • S3 object keys■ ■ • JWT secrets ■ ■ • Attestation ■ ■
■ ■ • Backup keys ■ ■ • mTLS certs ■ ■ • Merkle roots ■ ■
■ ■■■■■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■■■ ■
■ ■
■ KEY PROPERTIES ■
■ ■■■ Algorithm: AES-256-GCM (data), RSA-4096/ECDSA P-384 (signing) ■
■ ■■■ Rotation: Automatic (90 days data, 365 days root) ■
■ ■■■ Storage: AWS KMS (cloud), HSM (blockchain validators) ■
■ ■■■ Access: IAM policies, key policies, grants ■
■ ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

3.3.2 Encryption Standards

Data State	Encryption Method	Key Management	Standard
At Rest (Database)	AES-256-GCM	AWS KMS CMK	FIPS 197
At Rest (S3)	SSE-KMS	AWS KMS CMK	FIPS 197
At Rest (Backups)	AES-256-GCM	KMS + offline	FIPS 197
In Transit (External)	TLS 1.3	ACM certificates	RFC 8446
In Transit (Internal)	mTLS	Private CA	RFC 8446
In Transit (Blockchain)	Noise Protocol	Validator keys	Noise Framework
In Use (Sensitive Fields)	AES-256-GCM	Envelope encryption	FIPS 197

3.3.3 Sensitive Data Classification

Classification	Examples	Encryption	Access Control
Critical	Validator private keys	HSM-only	Physical + logical
Confidential	PII, transaction data	Field-level	Need-to-know

Internal	Rule definitions, configs	Volume-level	Role-based
Public	API schemas, documentation	None	Open access

4. Monitoring & Forensics Strategy

4.1 Security Monitoring Architecture

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ SECURITY MONITORING STACK ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ DATA SOURCES PROCESSING OUTPUTS ■
■ ■■■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■ ■
■ ■ CloudTrail ■■■■■■■■■■■■■■■■■■ ■ ■ Security ■ ■
■ ■ (API activity) ■ ■ ■ ■ Dashboard ■ ■
■ ■■■■■■■■■■■■■■■■■■■ ■ ■ ■■■■■■■■■■■■■■■ ■
■ ■■■■■■■■■■■■■■■■■■■ ■ ■ ■■■■■■■■■■■■■■■ ■
■ ■ VPC Flow Logs ■■■■■■■■■■■■■■■■■■ SIEM ■■■■■■ Alert ■ ■
■ ■ (network) ■ ■ (Splunk/ ■ ■ Management ■ ■
■ ■■■■■■■■■■■■■■■■■■■ ■ Sentinel) ■ ■■■■■■■■■■■■■■■ ■
■ ■■■■■■■■■■■■■■■■■■■ ■ ■ ■■■■■■■■■■■■■■■ ■
■ ■ Application Logs■■■■■■■■■■■■■■■■■■ ■■■■■■ Incident ■ ■
■ ■ (structured) ■ ■ ■ ■ Response ■ ■
■ ■■■■■■■■■■■■■■■■■■■ ■ ■ ■■■■■■■■■■■■■■■ ■
■ ■■■■■■■■■■■■■■■■■■■ ■ ■ ■■■■■■■■■■■■■■■ ■
■ ■ GuardDuty ■■■■■■■■■■■■■■■■■■ ■■■■■■ Threat ■ ■
■ ■ (threat intel) ■ ■ ■ ■ Hunting ■ ■
■ ■■■■■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■ ■■■■■■■■■■■■■■■ ■
■ ■■■■■■■■■■■■■■■■■■■ ■
■ ■ Blockchain Logs ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■ (consensus) ■ ■ Immutable ■ ■
■ ■■■■■■■■■■■■■■■■■■■ ■ Audit Trail ■ ■
■ ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

4.2 Detection Rules

Rule ID	Detection	Data Source	Response	SLA
D-001	Failed auth > 5 in 1min	CloudTrail	Account lockout	Immediate
D-002	Privilege escalation attempt	CloudTrail	Alert + block	5 minutes
D-003	Unusual data access pattern	App logs	Alert + review	15 minutes
D-004	Rule modification outside hours	App logs	Alert + approval hold	Immediate
D-005	Validator node offline	Blockchain	Alert + failover	1 minute
D-006	Consensus disagreement	Blockchain	Alert + investigation	Immediate
D-007	AI confidence anomaly	AI logs	Alert + human review	5 minutes
D-008	Lateral movement pattern	VPC Flow	Alert + isolation	5 minutes
D-009	Data exfiltration signature	VPC Flow	Block + alert	Immediate

D-010	Supply chain indicator	GuardDuty	Alert + containment	15 minutes

4.3 Forensics Capabilities

4.3.1 Evidence Collection

Evidence Type	Retention	Storage	Integrity
CloudTrail Logs	7 years	S3 (immutable)	SHA-256 hash chain
Application Logs	3 years	CloudWatch + S3	Log stream digest
Database Audit Logs	7 years	S3 (WORM)	Blockchain anchor
Network Captures	90 days	S3 (encrypted)	Packet timestamps
Blockchain State	Permanent	Distributed ledger	Consensus proof
Memory Dumps	On-demand	Encrypted S3	Chain of custody

4.3.2 Investigation Workflow

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ FORENSIC INVESTIGATION WORKFLOW ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ 1. DETECTION ■
■ ■■■ Security alert triggered ■
■ ■■■ Automated triage and severity assignment ■
■ ■
■ 2. CONTAINMENT ■
■ ■■■ Isolate affected systems (network segmentation) ■
■ ■■■ Preserve evidence (snapshot, memory dump) ■
■ ■■■ Notify incident response team ■
■ ■
■ 3. COLLECTION ■
■ ■■■ Gather logs from all relevant sources ■
■ ■■■ Export blockchain attestations for affected period ■
■ ■■■ Capture network traffic (if ongoing) ■
■ ■
■ 4. ANALYSIS ■
■ ■■■ Timeline reconstruction ■
■ ■■■ Attack vector identification ■
■ ■■■ Impact assessment ■
■ ■■■ Root cause determination ■
■ ■
■ 5. REMEDIATION ■
■ ■■■ Patch vulnerability / revoke access ■
■ ■■■ Restore from known-good state ■
■ ■■■ Verify system integrity ■
■ ■
■ 6. REPORTING ■
```

4.4 Immutable Audit Trail

PACT's blockchain layer provides tamper-evident logging:

```
Every Compliance Decision:
■■■ Transaction hash (unique identifier)
■■■ Decision details (rule, outcome, timestamp)
■■■ AI analysis hash (if AI was consulted)
■■■ Human approval hash (if required)
■■■ Merkle root (batch anchor)
■■■ Block signature (validator attestation)

Verification Process:
1. Retrieve attestation by transaction ID
```

```
2. Verify hash matches attestation content

3. Obtain Merkle proof from block

4. Verify block signature against validator registry

5. Confirm block is part of canonical chain
```

5. NIST 800-53 & CIS Controls Mapping

5.1 NIST 800-53 Rev 5 Control Mapping

Control Family	Control ID	Control Name	PACT Implementation
Access Control	AC-2	Account Management	Cognito + IAM with lifecycle automation
	AC-3	Access Enforcement	RBAC at API, service, and data layers
	AC-4	Information Flow	VPC segmentation, security groups
	AC-6	Least Privilege	Granular IAM policies, JIT access
	AC-17	Remote Access	VPN + mTLS, MFA required
Audit	AU-2	Event Logging	CloudTrail, app logs, blockchain
	AU-3	Content of Records	Structured JSON, full context
	AU-6	Audit Review	SIEM correlation, alerts
	AU-9	Protection of Audit	S3 WORM, blockchain immutability

	AU-10	Non-repudiation	Digital signatures, attestations
Config Management	CM-2	Baseline Configuration	CDK IaC, drift detection
	CM-3	Configuration Change Control	GitOps, PR approval workflow
	CM-6	Configuration Settings	CIS benchmarks enforced
	CM-8	System Component Inventory	AWS Config, asset management
Contingency	CP-9	System Backup	Automated backups, cross-region
	CP-10	Recovery and Reconstitution	RTO 4hr, RPO 1hr
Identification	IA-2	Multi-Factor Authentication	Hardware tokens for privileged
	IA-5	Authenticator Management	Secrets Manager, rotation
	IA-8	Identification of Non-Org Users	API keys with scoping
Incident Response	IR-4	Incident Handling	Automated playbooks
	IR-5	Incident Monitoring	24/7 SOC coverage
	IR-6	Incident Reporting	Regulatory notification workflow
Maintenance	MA-4	Non-Local Maintenance	Session recording, approval
Risk Assessment	RA-3	Risk Assessment	Quarterly threat modeling
	RA-5	Vulnerability Scanning	Daily automated scans
System Protection	SC-7	Boundary Protection	WAF, Shield, network ACLs

	SC-8	Transmission Confidentiality	TLS 1.3 everywhere
	SC-12	Cryptographic Key Management	KMS + HSM
	SC-13	Cryptographic Protection	FIPS 140-2 validated
	SC-28	Protection of Information at Rest	AES-256 encryption
Integrity	SI-3	Malware Protection	GuardDuty, container scanning
	SI-4	System Monitoring	SIEM, anomaly detection
	SI-7	Software Integrity	Code signing, SBOM

5.2 CIS Controls v8 Mapping

CIS Control	Control Name	PACT Implementation	Maturity
1	Inventory and Control of Enterprise Assets	AWS Config, asset tags	IG2
2	Inventory and Control of Software Assets	SBOM, container manifests	IG2
3	Data Protection	Classification, encryption	IG3
4	Secure Configuration	CIS benchmarks, IaC	IG2
5	Account Management	IAM automation, reviews	IG2
6	Access Control Management	RBAC, least privilege	IG3
7	Continuous Vulnerability Management	Daily scanning, patching	IG2

8	Audit Log Management	Centralized SIEM, retention	IG3
9	Email and Web Browser Protections	N/A (no email/browser)	-
10	Malware Defenses	Container scanning, GuardDuty	IG2
11	Data Recovery	Cross-region backups, testing	IG2
12	Network Infrastructure Management	VPC design, segmentation	IG2
13	Network Monitoring and Defense	VPC Flow, GuardDuty, WAF	IG3
14	Security Awareness Training	Annual training, phishing tests	IG1
15	Service Provider Management	Vendor assessments, contracts	IG2
16	Application Software Security	SAST, DAST, pen testing	IG3
17	Incident Response Management	Playbooks, tabletop exercises	IG2
18	Penetration Testing	Annual third-party testing	IG3

6. Blockchain Attack Surface

6.1 PoA Validator Compromise

6.1.1 Threat Description

In PACT's Proof-of-Authority consensus, validators are known entities (banks, regulators) that sign blocks. Compromising validator keys could allow:

- Block manipulation (reordering, censorship)
- False attestation injection
- Consensus disruption

6.1.2 Attack Vectors

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ VALIDATOR COMPROMISE VECTORS ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ VECTOR 1: KEY THEFT ■
■ ■■■ Physical HSM theft ■
■ ■■■ Remote HSM exploitation ■
■ ■■■ Insider key export ■
■ ■■■ Backup key compromise ■
■ ■
■ VECTOR 2: OPERATIONAL COMPROMISE ■
■ ■■■ Validator node malware ■
■ ■■■ Network interception (MITM) ■
■ ■■■ Configuration manipulation ■
■ ■■■ Software supply chain attack ■
■ ■
■ VECTOR 3: GOVERNANCE ATTACK ■
■ ■■■ Social engineering of operators ■
■ ■■■ Collusion between validators ■
■ ■■■ Regulatory capture ■
■ ■■■ Economic coercion ■
■ ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

6.1.3 Mitigations

Mitigation	Implementation	Effectiveness
Threshold Signatures	3-of-5 multi-sig for critical operations	High
HSM Key Storage	FIPS 140-3 Level 3 HSMs	High
Geographic Distribution	Validators in different jurisdictions	Medium
Slashing Conditions	Economic penalties for misbehavior	Medium
Validator Rotation	Annual re-election process	Medium
Watchdog Nodes	Non-signing observers monitoring consensus	High
Cryptographic Diversity	Multiple signature schemes	Medium

6.2 Attestation Fraud

6.2.1 Threat Description

Attackers may attempt to create false attestations claiming:

- Compliance checks that never occurred
- AI analyses that were never performed
- Human approvals that were never given

6.2.2 Attack Vectors

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■

■ ATTESTATION FRAUD VECTORS ■

■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■

■ ■

■ VECTOR 1: ATTESTATION FORGERY ■

■ ■■■ Signing key compromise ■

■ ■■■ Weak signature verification ■

■ ■■■ Replay of valid attestations ■
■ ■
■ VECTOR 2: CONTENT MANIPULATION ■
■ ■■■ Hash collision attacks ■
■ ■■■ Pre-image attacks on hashes ■
■ ■■■ Input data manipulation before hashing ■
■ ■
■ VECTOR 3: PROCESS BYPASS ■
■ ■■■ Direct database insertion ■
■ ■■■ API exploitation ■
■ ■■■ Time-of-check/time-of-use (TOCTOU) ■
■ ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

6.2.3 Mitigations

Mitigation	Implementation	Effectiveness
Hash Chaining	SHA-256 chain linking attestations	High
Timestamp Authority	RFC 3161 trusted timestamps	High
Multi-Source Verification	Independent attestation from multiple services	High
Merkle Tree Batching	Efficient verification of attestation sets	High
Blockchain Anchoring	Immutable record of Merkle roots	Critical
Randomized Auditing	Spot-check attestations against source systems	Medium

6.3 Oracle Poisoning

6.3.1 Threat Description

PACT depends on external data feeds (oracles) for:

- Sanctions lists (OFAC SDN)
- Regulatory updates
- Market data for risk calculations
- Identity verification services

Poisoned oracle data could cause incorrect compliance decisions.

6.3.2 Attack Vectors

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ORACLE POISONING VECTORS ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ VECTOR 1: SOURCE COMPROMISE ■
■ ■■■ Hack of authoritative data provider ■
■ ■■■ Insider manipulation at source ■
■ ■■■ DNS hijacking of data endpoints ■
■ ■
■ VECTOR 2: TRANSPORT MANIPULATION ■
■ ■■■ MITM attack on data feed ■
■ ■■■ Cache poisoning ■
■ ■■■ Delayed/stale data injection ■
■ ■
■ VECTOR 3: PROCESSING EXPLOITATION ■
■ ■■■ Parser vulnerabilities ■
■ ■■■ Format string attacks ■
■ ■■■ Deserialization exploits ■
■ ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

6.3.3 Mitigations

Mitigation	Implementation	Effectiveness

Multi-Oracle Consensus	Require agreement from 2+ independent sources	High
Cryptographic Verification	Signed data from authoritative sources	High
Anomaly Detection	Alert on unexpected data changes	Medium
Rate Limiting	Prevent rapid data churn attacks	Medium
Historical Comparison	Compare against known-good baselines	Medium
Manual Override Queue	Flag suspicious updates for human review	High

7. Risk Mitigation Strategies

7.1 Risk Treatment Matrix

Risk	Likelihood	Impact	Treatment	Residual Risk
Validator Compromise	Low	Critical	Threshold signatures, HSM, monitoring	Low
Attestation Fraud	Medium	High	Hash chains, blockchain anchoring	Low
Oracle Poisoning	Medium	High	Multi-source, signing, anomaly detection	Low
AI Model Manipulation	Low	High	Human oversight, confidence thresholds	Low

Data Exfiltration	Medium	Critical	Encryption, DLP, access controls	Medium
Insider Threat	Medium	High	Separation of duties, audit logging	Medium
Supply Chain Attack	Low	Critical	SBOM, signing, vulnerability scanning	Low
DDoS	High	Medium	Shield Advanced, auto-scaling	Low

7.2 Defense-in-Depth Summary

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ DEFENSE-IN-DEPTH LAYERS ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ LAYER 1: PREVENTIVE CONTROLS ■
■ ■■■ Network segmentation and firewalls ■
■ ■■■ Strong authentication (MFA, mTLS) ■
■ ■■■ Encryption (at rest and in transit) ■
■ ■■■ Input validation and sanitization ■
■ ■■■ Least privilege access ■
■ ■
■ LAYER 2: DETECTIVE CONTROLS ■
■ ■■■ Continuous monitoring (SIEM) ■
■ ■■■ Anomaly detection (ML-based) ■
■ ■■■ Threat intelligence integration ■
■ ■■■ Vulnerability scanning ■
■ ■■■ Blockchain consensus monitoring ■
■ ■
■ LAYER 3: CORRECTIVE CONTROLS ■
■ ■■■ Automated incident response ■
■ ■■■ System isolation capabilities ■
■ ■■■ Backup and recovery ■
■ ■■■ Patch management ■
■ ■■■ Key revocation procedures ■
■ ■
■ LAYER 4: RECOVERY CONTROLS ■
■ ■■■ Business continuity planning ■
■ ■■■ Disaster recovery (multi-region) ■
■ ■■■ Data restoration from immutable backups ■
■ ■■■ Blockchain state recovery ■
```

7.3 Incident Response Plan

Phase	Actions	Timeline	Owner
Detection	Alert triage, severity classification	< 15 min	SOC
Containment	Isolate affected systems, preserve evidence	< 1 hour	IR Team
Eradication	Remove threat, patch vulnerability	< 24 hours	Engineering
Recovery	Restore services, verify integrity	< 48 hours	Operations
Lessons Learned	Root cause analysis, control updates	< 2 weeks	Security

8. Compliance Certifications Roadmap

8.1 Current Status

Certification	Status	Target Date
SOC 2 Type I	In Progress	Q1 2025
SOC 2 Type II	Planned	Q3 2025
FedRAMP Moderate	Assessment	Q4 2025
FedRAMP High	Planned	Q2 2026
ISO 27001	Planned	Q4 2025
PCI DSS	Assessment	Q2 2025

8.2 Third-Party Assessments

Assessment Type	Frequency	Last Completed	Next Scheduled
Penetration Testing	Annual	N/A	Q1 2025
Vulnerability Assessment	Quarterly	N/A	Q1 2025
Code Security Audit	Annual	N/A	Q1 2025
Architecture Review	Annual	N/A	Q1 2025
Red Team Exercise	Annual	N/A	Q2 2025

9. Conclusion

The PACT Protocol implements a comprehensive, defense-in-depth security architecture designed to protect the integrity, confidentiality, and availability of compliance operations. Key security properties include:

1. **Zero Trust**: No implicit trust; every request authenticated and authorized
2. **Immutable Audit Trail**: Blockchain-anchored attestations that cannot be tampered with
3. **Defense in Depth**: Multiple layers of preventive, detective, and corrective controls
4. **Regulatory Alignment**: Full mapping to NIST 800-53 and CIS Controls
5. **Blockchain Security**: Specific mitigations for PoA, attestation, and oracle threats

The architecture is designed for continuous improvement through regular threat modeling, penetration testing, and control assessments.

Appendix A: Security Contact Information

Security Team: security@arkasystems.com

Vulnerability Disclosure: https://arkasystems.com/security/disclosure

24/7 Security Operations Center: [Contact details provided under NDA]

Appendix B: Document Control

Version	Date	Author	Changes
1.0	December 2024	Security Engineering	Initial release

Next Review: March 2025

Classification: CISO Reference Document

This document is prepared for security evaluation by qualified information security professionals. ARKA Systems LLC welcomes detailed technical examination of all security claims made herein.