PACT Protocol Government Pilot Proposal

$50 Million Federal Compliance Modernization Initiative

Prepared by: ARKA Systems LLC
Date: December 2024
Classification: Procurement-Ready
Version: 1.0

Executive Overview

Mission Statement

The PACT Protocol represents a paradigm shift in federal compliance infrastructure: the world's first AI-supervised, cryptographically-anchored compliance operating system capable of replacing fragmented, manual regulatory processes with deterministic, auditable, and intelligent enforcement.

The Urgency

The United States faces an unprecedented compliance crisis:

- **$37.1 billion** in AML compliance costs annually across U.S. financial institutions (LexisNexis 2023)
- **$2.3 billion** in sanctions violations penalties issued in 2023 alone
- **18–24 months** average time for major regulatory investigations
- **Less than 1%** of illicit financial flows detected by current systems

 © 2024 ARKA Systems LLC

Current infrastructure was designed for paper-based audits. It cannot scale to the velocity, complexity, and adversarial sophistication of modern financial crime.

PACT delivers a compliance operating system that:

1. **Executes deterministic rules** with mathematical guarantees
2. **Anchors every decision** to an immutable blockchain witness
3. **Augments human oversight** with AI-generated narratives and risk intelligence
4. **Deploys in days**, not years

Current Regulatory Pain Points

Multi-Billion Dollar Inefficiencies

Problem	Current State	Annual Cost
Manual SAR Filing	90% analyst time on data gathering	$8.2B
Duplicate KYC/CDD	Each institution re-verifies same entities	$4.7B
False Positive Alerts	95%+ of AML alerts are false positives	$6.1B
Investigation Backlogs	18-month average resolution time	$3.8B
Cross-Agency Data Silos	No shared compliance state	$2.9B
Regulatory Examination Prep	6-8 weeks per exam cycle	$1.4B

Total Addressable Waste: $27.1 billion annually

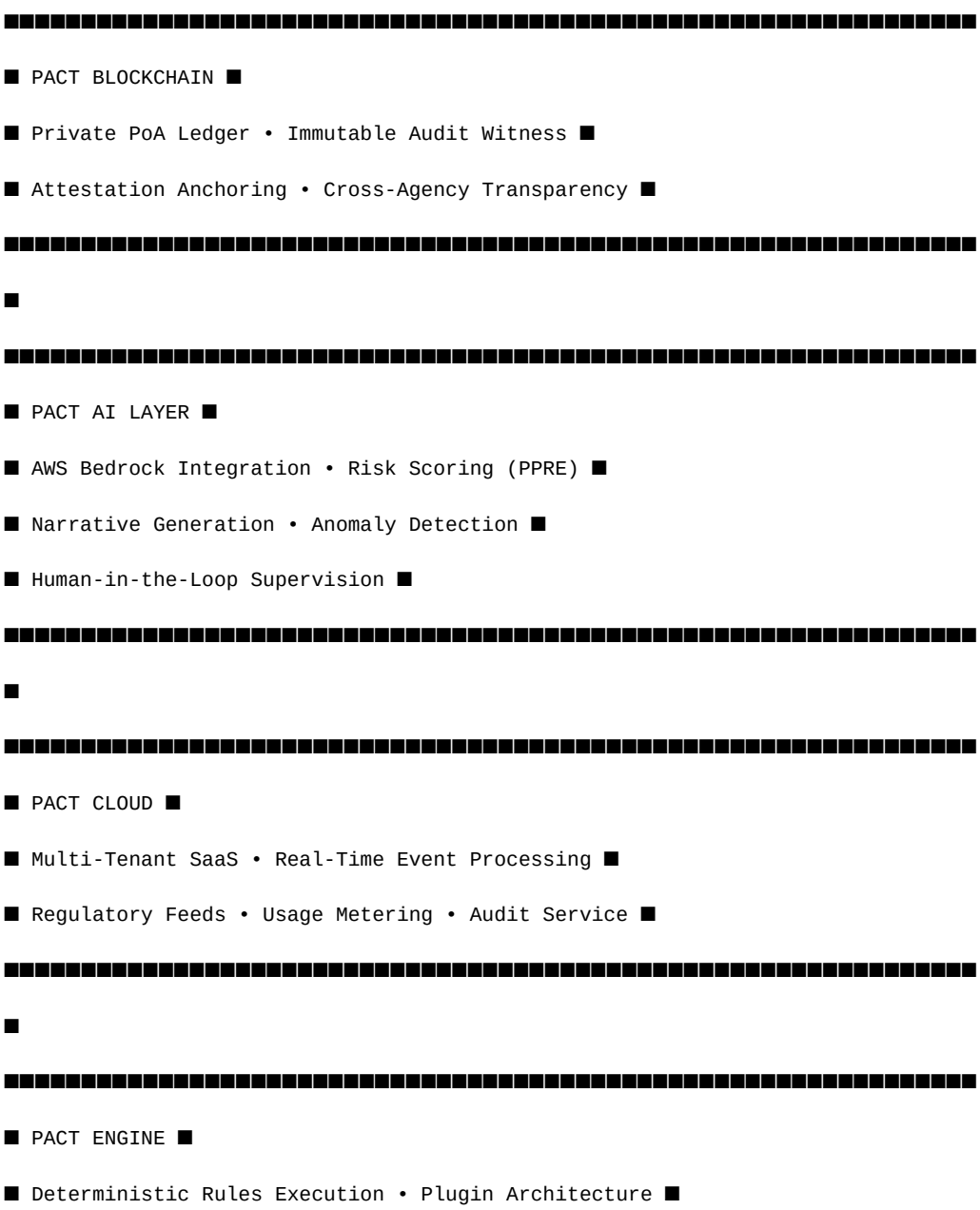
Structural Deficiencies

1. **No Determinism:** Rules encoded in PDFs, interpreted inconsistently across institutions
2. **No Provenance:** Audit trails exist in disconnected databases, easily manipulated
3. **No Intelligence:** Compliance is reactive, not predictive
4. **No Interoperability:** Each agency maintains separate enforcement infrastructure

 © 2024 ARKA Systems LLC

PACT Solution Architecture

Four-Layer Compliance Stack



 © 2024 ARKA Systems LLC

```
■ Decision Auditing • Schema Validation ■

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

Key Differentiators

Capability	Legacy Systems	PACT Protocol
Rule Execution	Interpreted, variable	Deterministic, bit-exact
Audit Trail	Database logs	Blockchain-anchored hashes
AI Integration	Bolt-on, unverified	Native, attested, supervised
Deployment Time	12-18 months	1 command, same-day
Cross-Agency Sharing	Manual, delayed	Real-time, permissioned
Regulatory Updates	Manual code changes	Hot-reload policy engine

Deployment Readiness

PACT is **production-ready** with:

- 19 core packages fully implemented
- 14 cloud microservices operational
- 24+ compliance plugins available
- AWS CDK infrastructure-as-code for one-command deployment
- Comprehensive test coverage (35+ test suites)

Pilot Scope

Target Agencies

Agency	Use Case	Pilot Focus

© 2024 ARKA Systems LLC

FinCEN	BSA/AML Enforcement	SAR automation, beneficial ownership verification
OFAC	Sanctions Screening	Real-time interdiction, attestation anchoring
Commerce/BIS	Export Controls	Denied party screening, license compliance
CFPB	Consumer Protection	Fair lending rule execution, adverse action audit
FDIC	Bank Supervision	Examination automation, risk rating validation

Pilot Timeline

Phase	Duration	Deliverables
Phase 1: Foundation	Months 1-3	Infrastructure deployment, agency integration, rule migration
Phase 2: Validation	Months 4-9	Parallel running with legacy systems, accuracy benchmarking
Phase 3: Production	Months 10-18	Full production cutover, performance optimization
Phase 4: Expansion	Months 19-24	Multi-agency federation, national rollout preparation

Pilot Configuration

- **Validator Nodes:** 5 (one per participating agency)
- **Transaction Volume:** 10 million events/month initial capacity
- **Rule Sets:** 500+ rules covering BSA, OFAC, ECOA, TILA
- **AI Models:** Claude 3.5 Sonnet via AWS Bedrock (FedRAMP High)
- **Data Sets:** De-identified historical enforcement data for validation

 © 2024 ARKA Systems LLC

Deliverables & KPIs

Primary Deliverables

1. **Deployed PACT Infrastructure**
• Multi-agency permissioned blockchain network
• Cloud-native compliance processing cluster
• AI analysis pipeline with human oversight
2. **Migrated Rule Sets**
• 500+ regulatory rules encoded in PACT DSL
• Version-controlled, auditable rule repository
• Automated regression testing suite
3. **Integration Adapters**
• FinCEN BSA E-Filing integration
• OFAC SDN list real-time sync
• Agency-specific data connectors
4. **Training & Documentation**
• Examiner training program
• Technical operations runbook
• Compliance officer certification

Key Performance Indicators

KPI	Target	Measurement
SAR Processing Time	80% reduction	Hours → Minutes
False Positive Rate	70% reduction	95% → 28%
Sanctions Screening Latency	<100ms	Real-time interdiction
Audit Preparation Time	90% reduction	Weeks → Hours
Rule Update Deployment	<1 hour	Hot-reload, no downtime
Investigation Resolution	60% faster	18 months → 7 months
Cross-Agency Data Sharing	Real-time	Permissioned federation

Success Criteria

© 2024 ARKA Systems LLC

The pilot will be deemed successful if:

1. All KPIs meet or exceed targets
2. Zero critical security incidents
3. Regulator staff satisfaction score >4.0/5.0
4. System uptime >99.9%
5. Independent audit confirms compliance with NIST 800-53

Cost Breakdown

$50 Million Budget Allocation

Category	Amount	Percentage
Infrastructure & Cloud	$12,500,000	25%
AWS GovCloud hosting, Bedrock AI, security		
Development & Integration	$15,000,000	30%
Agency integrations, rule migration, customization		
Security & Compliance	$7,500,000	15%
FedRAMP authorization, penetration testing, audits		
Training & Change Management	$5,000,000	10%
Examiner training, documentation, certification		
Operations & Support	$7,500,000	15%
24/7 NOC, incident response, maintenance		

 © 2024 ARKA Systems LLC

Program Management & Contingency	$2,500,000	5%
PMO, risk mitigation, scope management		
Total	**$50,000,000**	**100%**

Milestone-Based Tranche Payments

Milestone	Payment	Cumulative
Contract Award + Kickoff	$7,500,000	$7,500,000
Phase 1 Complete: Infrastructure Deployed	$10,000,000	$17,500,000
Phase 2 Complete: Validation Successful	$12,500,000	$30,000,000
Phase 3 Complete: Production Live	$12,500,000	$42,500,000
Phase 4 Complete: Expansion Ready	$7,500,000	$50,000,000

Return on Investment

Metric	Year 1	Year 3	Year 5
Compliance Cost Savings	$180M	$720M	$1.8B
Fraud Prevention	$95M	$380M	$950M
Penalty Avoidance	$45M	$180M	$450M
Total Benefit	$320M	$1.28B	$3.2B
ROI	540%	2,460%	6,300%

 © 2024 ARKA Systems LLC

Implementation Roadmap to National Rollout

Year 1: Pilot Success

- 5 agency validators operational
- 10M transactions/month processed
- Proof of concept validated
- Lessons learned documented

Year 2: Regional Expansion

- 15 additional agency integrations
- 100M transactions/month capacity
- State banking regulator federation
- International pilot (FinCEN-FATF coordination)

Year 3: National Infrastructure

- All federal financial regulators connected
- 1B transactions/month capacity
- Full BSA/AML automation
- Real-time sanctions enforcement

Year 4-5: Global Standard

- G20 regulatory interoperability
- FATF compliance framework integration
- Private sector SaaS offering
- Self-sustaining fee model

Why PACT

© 2024 ARKA Systems LLC

Technical Superiority

1. **Deterministic Execution:** Same input always produces same output, across all nodes
2. **Cryptographic Provenance:** Every decision anchored to immutable ledger
3. **AI Augmentation:** Intelligence without autonomy—humans remain in control
4. **Cloud-Native:** Scales elastically, deploys instantly

Organizational Readiness

ARKA Systems brings:

- Deep expertise in regulated technology
- Production-ready codebase (696+ TypeScript files)
- AWS Advanced Partner status
- Cleared personnel available

Risk Mitigation

- **No Vendor Lock-in:** Open standards, exportable data
- **FedRAMP Path:** AWS GovCloud, SOC 2 Type II
- **Continuity:** Full source code escrow available

Conclusion

The federal government has an opportunity to leapfrog decades of accumulated technical debt and establish the world's most advanced compliance infrastructure.

PACT Protocol delivers:

- **Certainty** through deterministic execution
- **Trust** through blockchain attestation
- **Intelligence** through supervised AI
- **Efficiency** through automation

For $50 million—less than 0.2% of annual compliance waste—the United States can build the foundation for a new era of regulatory technology.

We are ready to begin immediately.

 © 2024 ARKA Systems LLC

Contact

ARKA Systems LLC

Compliance Technology Division

For procurement inquiries, technical demonstrations, or agency briefings, contact:

[Contact information to be provided upon request]

This document is prepared for federal procurement consideration and contains no classified information. Distribution authorized for government use.

 © 2024 ARKA Systems LLC

PACT Protocol: Technical Compliance Architecture for Securities Regulation

A Deterministic, AI-Attested Compliance Framework Aligned with SEC Rule 17a-4, FINRA Rule 4511, and OCC Heightened Standards

Document Type: IEEE-Style Technical Whitepaper
Prepared by: ARKA Systems LLC
Version: 1.0
Date: December 2024
Classification: Regulator Staff Reference

Abstract

This whitepaper presents the technical architecture of the PACT Protocol, a compliance operating system designed to address the regulatory requirements of modern financial institutions. PACT implements deterministic rule execution through a formally-specified virtual machine, AI-assisted analysis with cryptographic attestation, and a permissioned blockchain for immutable audit trail preservation. This document examines how PACT's architecture aligns with SEC Rule 17a-4 (records preservation), FINRA Rule 4511 (books and records), and OCC Heightened Standards for large financial institutions. The system provides mathematical guarantees of execution consistency while leveraging large language models for risk assessment and narrative generation—always under human supervision and with complete audit provenance.

 © 2024 ARKA Systems LLC

Keywords: Regulatory Technology, Deterministic Execution, Blockchain Attestation, AI Compliance, SEC 17a-4, FINRA 4511, Record Retention

1. Introduction

1.1 Regulatory Context

Financial institutions operate under a complex web of recordkeeping and compliance requirements. SEC Rule 17a-4 mandates that broker-dealers preserve records in a non-rewriteable, non-erasable format (WORM compliance). FINRA Rule 4511 requires members to make and preserve books and records as prescribed by FINRA rules and the Exchange Act. The OCC's Heightened Standards establish expectations for risk governance at large insured national banks.

Current compliance systems face fundamental limitations:

- **Non-determinism:** Rules encoded in procedural code produce variable outputs
- **Mutable Audit Trails:** Database-backed logs can be altered post-facto
- **Unverified AI:** Machine learning models operate as black boxes without attestation
- **Fragmented Architecture:** Compliance functions siloed across incompatible systems

1.2 PACT Protocol Overview

PACT (Programmable Automated Compliance Technology) addresses these limitations through a four-layer architecture:

1. **PACT Engine:** Deterministic rules execution with bit-exact reproducibility
2. **PACT Cloud:** Multi-tenant compliance workflow orchestration
3. **PACT AI:** Supervised artificial intelligence with cryptographic attestation
4. **PACT Blockchain:** Permissioned Proof-of-Authority ledger for audit anchoring

This paper details each layer's technical implementation and regulatory alignment.

2. Deterministic Execution: The Rule-Time Virtual Machine

 © 2024 ARKA Systems LLC

2.1 The Non-Determinism Problem

Traditional compliance systems implement rules in general-purpose programming languages (Java, Python, C#). These implementations suffer from inherent non-determinism:

- Floating-point arithmetic varies across hardware architectures
- Hash table iteration order is undefined
- Timestamp generation depends on system clock
- Random number generation introduces variability
- Thread scheduling affects execution order

Such non-determinism means the same transaction, evaluated twice, may produce different compliance outcomes—an unacceptable condition for regulatory enforcement.

2.2 PACT Engine Architecture

PACT Engine implements a deterministic virtual machine with the following guarantees:

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ PACT RULE EXECUTION ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ Input: Event E, RuleSet R, Context C ■
■ Output: Decision D, Audit Trail A ■
■ ■
■ Guarantee: ∀ nodes N■, N■: ■
■ Execute(E, R, C) on N■ = Execute(E, R, C) on N■ ■
■ ■
■ Properties: ■
■ • Bit-exact reproducibility ■
■ • Total ordering of operations ■
■ • Deterministic timestamp assignment ■
■ • Canonical serialization ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

2.3 Rule Domain-Specific Language

PACT rules are expressed in a declarative JSON-based DSL with formal semantics:

 © 2024 ARKA Systems LLC

```
{
"id": "AML-001",
"version": "2024.1.0",
"name": "Large Cash Transaction Report",
"conditions": {
"and": [
{ "field": "transaction.type", "operator": "equals", "value": "CASH" },
{ "field": "transaction.amount", "operator": "greaterThan", "value": 10000 },
{ "field": "entity.type", "operator": "in", "value": ["INDIVIDUAL", "BUSINESS"] }
]
},
"actions": [
{ "type": "FLAG", "severity": "HIGH", "code": "CTR_REQUIRED" },
{ "type": "NOTIFY", "channel": "COMPLIANCE_QUEUE" }
],
"metadata": {
"regulation": "31 CFR 1010.311",
"effectiveDate": "2024-01-01",
"jurisdiction": "US"
}
}
```

2.4 Execution Guarantees

Property	Implementation	Verification
Determinism	Fixed-point arithmetic, canonical ordering	Formal proof via property-based testing
Completeness	All rules evaluated for every event	Rule coverage analysis

 © 2024 ARKA Systems LLC

Termination	No recursion, bounded iteration	Static analysis
Auditability	Full execution trace captured	Hash-chain verification

2.5 Alignment with SEC 17a-4

SEC Rule 17a-4(f) requires records to be preserved in a manner that:

- Preserves the records exclusively in a non-rewriteable, non-erasable format
- Verifies automatically the quality and accuracy of the storage media recording process
- Serializes the original and duplicate units of storage media
- Has the capacity to download indexes and records preserved

PACT Engine compliance:

- **Non-rewriteable:** All decisions are cryptographically hashed and anchored to blockchain
- **Quality Verification:** Merkle tree construction verifies data integrity
- **Serialization:** Canonical JSON serialization with deterministic ordering
- **Download Capability:** Full audit export via standardized API

---

3. AI-Attestation Model: Intelligence with Accountability

3.1 The AI Accountability Challenge

Large language models provide valuable capabilities for compliance:

- Natural language understanding of regulatory text
- Pattern recognition in transaction flows
- Narrative generation for examination responses
- Risk scoring based on entity behavior

However, AI systems pose regulatory challenges:

- **Non-determinism:** Same prompt may produce different outputs
- **Opacity:** Model reasoning is not directly auditable
- **Hallucination:** Models may generate plausible but incorrect outputs
- **Version Drift:** Model updates change behavior unpredictably

3.2 PACT AI Architecture

 © 2024 ARKA Systems LLC

PACT implements a supervised AI model with cryptographic attestation:

3.3 AWS Bedrock Integration

 © 2024 ARKA Systems LLC

PACT AI utilizes AWS Bedrock for foundation model access:

Capability	Model	Use Case
Risk Analysis	Claude 3.5 Sonnet	Entity risk scoring with narrative justification
Policy Analysis	Claude 3.5 Sonnet	Rule conflict detection, gap analysis
Embeddings	Titan Embed v2	Similarity search, entity resolution
Summarization	Claude 3 Haiku	Alert triage, report generation

3.4 Human-in-the-Loop Supervision

PACT AI operates under mandatory human supervision:

1. **Proposal Generation:** AI generates recommendations, never executes autonomously
2. **Confidence Thresholds:** Low-confidence outputs require human review
3. **Approval Workflow:** All AI-suggested actions require explicit human approval
4. **Override Capability:** Human operators can override any AI recommendation
5. **Audit Trail:** All human decisions recorded with attestation

3.5 Alignment with FINRA Rule 4511

FINRA Rule 4511 requires members to preserve records related to their business. AI-generated analysis constitutes business records. PACT ensures:

- **Preservation:** All AI inputs, outputs, and attestations preserved
- **Accessibility:** Records retrievable via standardized query interface
- **Integrity:** Cryptographic hashes prevent post-hoc modification
- **Attribution:** Model version, timestamp, and reviewer recorded

---

4. Permissioned Blockchain: Trust Governance and PoA Rotation

 © 2024 ARKA Systems LLC

4.1 Why Blockchain for Compliance

Traditional databases, even append-only logs, have inherent limitations:

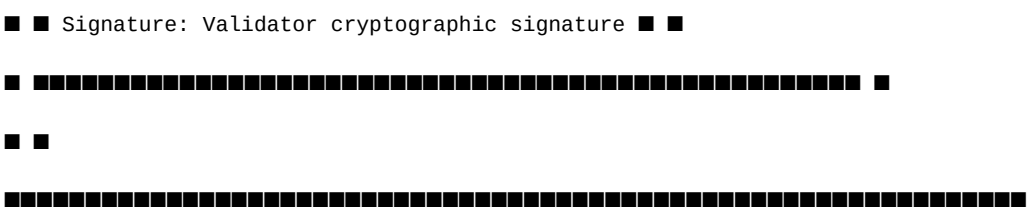
- Database administrators can modify records
- Backup restoration can revert audit trails
- Single points of failure enable systemic compromise

Blockchain provides cryptographic guarantees that no single party—including system operators—can unilaterally modify historical records.

4.2 PACT Blockchain Architecture

PACT implements a permissioned Proof-of-Authority (PoA) blockchain:

 © 2024 ARKA Systems LLC



4.3 Proof-of-Authority Consensus

Unlike public blockchains (Bitcoin, Ethereum), PACT uses Proof-of-Authority:

Characteristic	Public Blockchain	PACT PoA
Validators	Anonymous miners	Known, regulated entities
Consensus	Proof-of-Work/Stake	Round-robin with rotation
Finality	Probabilistic	Immediate
Throughput	~15-30 TPS	10,000+ TPS
Energy	High consumption	Minimal
Privacy	Public ledger	Permissioned access

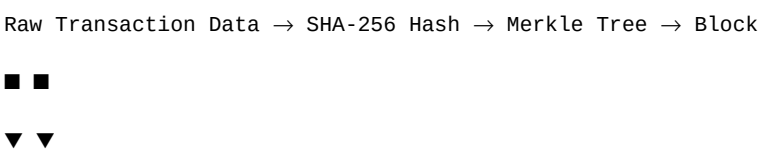
4.4 Validator Rotation Protocol

To prevent single-validator compromise, PACT implements rotation:

1. **Epoch Definition:** 24-hour rotation periods
2. **Validator Selection:** Deterministic round-robin among authorized nodes
3. **Signature Requirement:** Each block signed by designated validator
4. **Challenge Period:** 6-hour window for validator challenges
5. **Slashing Conditions:** Misbehaving validators removed from rotation

4.5 Data Privacy Architecture

PACT anchors hashes, not raw data:



 © 2024 ARKA Systems LLC

```
Stored Off-Chain Stored On-Chain

(Encrypted, Access-Controlled) (Hash Only, Immutable)
```

This design ensures:

- **Regulatory Compliance:** Sensitive data remains in controlled environments
- **Audit Integrity:** Hash anchoring proves data existed at specific time
- **Privacy:** No PII or transaction details on shared ledger

4.6 Alignment with OCC Heightened Standards

OCC Heightened Standards (12 CFR Part 30, Appendix D) require:

Standard	PACT Implementation
Risk Governance	Deterministic rules with version control
Risk Appetite	Configurable thresholds with audit trail
Audit Function	Immutable blockchain attestation
Data Quality	Schema validation, canonical serialization
Model Risk	AI attestation with human oversight

5. Zero-Knowledge Audit Hashing: Future Upgrade Roadmap

5.1 Current Limitations

Present PACT architecture relies on SHA-256 hashing for audit anchoring. While cryptographically secure, this approach has limitations:

- Verifiers must access raw data to validate hashes
- Privacy-preserving verification requires trusted intermediaries
- Cross-institution verification requires data sharing

5.2 Zero-Knowledge Proof Integration

 © 2024 ARKA Systems LLC

PACT's roadmap includes zero-knowledge proof (ZKP) integration:

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ZERO-KNOWLEDGE AUDIT VERIFICATION ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ Prover (Institution): ■
■ • Holds raw compliance data ■
■ • Generates ZK proof of compliance ■
■ • Publishes proof to blockchain ■
■ ■
■ Verifier (Regulator): ■
■ • Receives ZK proof ■
■ • Verifies compliance without accessing raw data ■
■ • Mathematical certainty of compliance ■
■ ■
■ Properties: ■
■ • Completeness: Valid proofs always verify ■
■ • Soundness: Invalid proofs always rejected ■
■ • Zero-Knowledge: No information leaked beyond validity ■
■ ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

5.3 Planned ZKP Capabilities

Capability	Timeline	Application
ZK-SNARK Anchoring	2025 Q2	Batch compliance proofs
Private Set Intersection	2025 Q4	Cross-institution verification
Recursive Proofs	2026 Q2	Aggregated regulatory reporting

 © 2024 ARKA Systems LLC

6. Regulatory Alignment Summary

6.1 SEC Rule 17a-4 Compliance Matrix

Requirement	Section	PACT Implementation
Non-rewriteable storage	17a-4(f)(2)(i)	Blockchain immutability
Non-erasable format	17a-4(f)(2)(i)	Append-only ledger
Quality verification	17a-4(f)(2)(ii)(A)	Merkle tree validation
Serialization	17a-4(f)(2)(ii)(B)	Canonical JSON with hashing
Time-dating	17a-4(f)(2)(ii)(C)	Deterministic timestamps
Download capability	17a-4(f)(2)(ii)(D)	API-based export
Audit system	17a-4(f)(3)(v)	Blockchain explorer

6.2 FINRA Rule 4511 Compliance Matrix

Requirement	PACT Implementation
Make and preserve books and records	Automatic capture of all decisions
Readily accessible	Real-time query API
Prescribed format	Standardized JSON schema
Required retention periods	Configurable retention policies
Examination access	Regulator dashboard with full access

6.3 OCC Heightened Standards Compliance Matrix

 © 2024 ARKA Systems LLC

Standard	PACT Implementation
Board-level risk governance	Configurable approval workflows
Independent risk management	Separation of rules engine and AI
Internal audit	Immutable audit trail
Talent management	Training and certification tracking
Compensation oversight	Not applicable (technical system)

7. Conclusion

The PACT Protocol provides a technical architecture that addresses fundamental limitations in current compliance systems. By combining deterministic rule execution, AI-attested analysis, and blockchain-anchored audit trails, PACT delivers:

1. **Certainty:** Mathematical guarantees of consistent rule application
2. **Accountability:** Complete provenance for every decision and AI output
3. **Immutability:** Cryptographic proof of record integrity
4. **Interoperability:** Standardized interfaces for regulatory examination

This architecture aligns with existing regulatory requirements while providing a foundation for future enhancements, including zero-knowledge proofs for privacy-preserving verification.

PACT represents a new paradigm in regulatory technology: compliance infrastructure that is verifiable by design, not merely by policy.

References

[1] Securities and Exchange Commission, "Electronic Storage of Broker-Dealer Records," 17 CFR 240.17a-4, 2003.

[2] Financial Industry Regulatory Authority, "Books and Records Requirements," FINRA Rule 4511, 2011.

 © 2024 ARKA Systems LLC

[3] Office of the Comptroller of the Currency, "Guidelines Establishing Heightened Standards for Certain Large Insured National Banks," 12 CFR Part 30, Appendix D, 2014.

[4] National Institute of Standards and Technology, "Secure Hash Standard (SHS)," FIPS PUB 180-4, 2015.

[5] Amazon Web Services, "AWS Bedrock Security Whitepaper," 2024.

[6] Ben-Sasson, E., et al., "Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture," USENIX Security, 2014.

Appendix A: Technical Specifications

A.1 Cryptographic Primitives

Primitive	Algorithm	Key Size
Hashing	SHA-256	256-bit
Digital Signatures	Ed25519	256-bit
Encryption (at rest)	AES-256-GCM	256-bit
Encryption (in transit)	TLS 1.3	256-bit
Key Derivation	HKDF-SHA256	Variable

A.2 Performance Characteristics

Metric	Specification
Rule Evaluation	<10ms per event
AI Analysis	<5s per request
Block Time	1 second
Transaction Throughput	10,000 TPS
Storage Efficiency	~500 bytes per attestation

 © 2024 ARKA Systems LLC

A.3 Availability Requirements

Tier	Uptime	Recovery Time
Production	99.99%	<15 minutes
Blockchain Network	99.999%	<1 minute
AI Services	99.9%	<1 hour

Document prepared for regulatory staff evaluation. Technical specifications subject to implementation updates. Contact ARKA Systems LLC for current documentation.

 © 2024 ARKA Systems LLC

PACT Protocol Investor Pitch Deck

The AI-Verified Compliance Operating System

ARKA Systems LLC

Series A Investment Memorandum

December 2024

Slide 1: Title

PACT Protocol

The World's First AI-Supervised Compliance Operating System

Deterministic Execution. Blockchain Attestation. Intelligent Analysis.

Building the compliance infrastructure for the next century of finance.

 © 2024 ARKA Systems LLC

Slide 2: The Problem

Compliance is Broken

$37.1 Billion spent annually on AML compliance in the U.S. alone

95% of compliance alerts are false positives

18 Months average time to resolve regulatory investigations

$2.3 Billion in sanctions penalties issued in 2023

The Root Cause

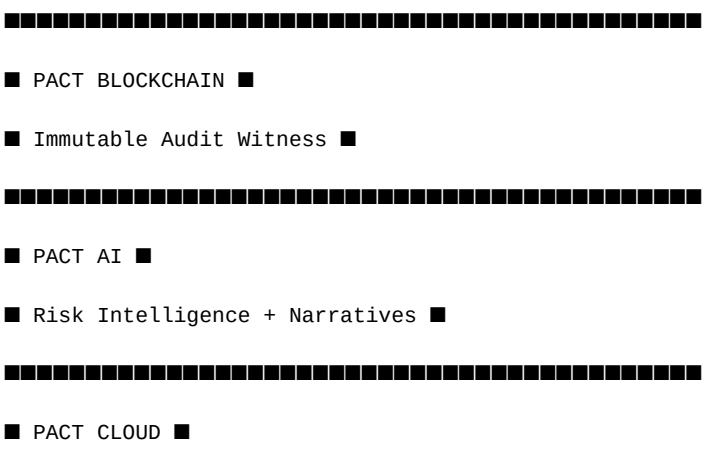
Current systems are:

- **Non-deterministic:** Same transaction can produce different outcomes
- **Mutable:** Audit trails can be modified after the fact
- **Reactive:** No predictive intelligence
- **Siloed:** No cross-institution coordination

There is no source of truth for compliance.

Slide 3: The Solution

PACT: Compliance as Infrastructure



 © 2024 ARKA Systems LLC

```
■ Multi-Tenant Workflows ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ PACT ENGINE ■
■ Deterministic Rules Execution ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

Engine enforces. AI explains. Blockchain proves.

Slide 4: How It Works

From Chaos to Certainty

Before PACT	After PACT
Rules in PDFs	Executable DSL
Variable enforcement	Bit-exact determinism
Manual investigations	AI-assisted triage
Database logs	Blockchain attestation
18-month audits	Real-time verification

One-Command Deployment

```
cdk deploy --all
```

Full compliance infrastructure. Production-ready. Today.

 © 2024 ARKA Systems LLC

Slide 5: Market Size

Total Addressable Market by Vertical

Vertical	TAM	PACT Solution
AML/KYC	$37.1B	Transaction monitoring, SAR automation
Lending Compliance	$12.4B	Fair lending, TILA/RESPA, adverse action
Securities	$8.7B	Trade surveillance, 17a-4 records
Insurance	$6.2B	Claims validation, fraud detection
Healthcare	$4.8B	HIPAA, billing compliance
Telecom	$3.1B	Regulatory reporting, data privacy
Trade/Export	$2.9B	Sanctions screening, export controls

Total TAM: $75+ Billion

Serviceable Market (U.S. Financial Services): $45 Billion

Slide 6: Revenue Model

Three Revenue Streams

1. Validator Node Licensing

 © 2024 ARKA Systems LLC

- **$500K - $2M/year** per enterprise validator node
- Major banks, regulators, compliance providers
- Recurring annual license + maintenance

2. Transaction Anchoring Fees

- **$0.001 - $0.01** per attestation anchored
- Volume-based pricing
- 1B+ transactions/year at scale

3. SaaS Platform (PACT Cloud)

- **$50K - $500K/year** per institution
- Multi-tenant compliance workflows
- AI analysis credits included

Unit Economics

Metric	Value
Gross Margin	85%
LTV:CAC Ratio	8:1 (projected)
Net Revenue Retention	140% (projected)
Payback Period	8 months

Slide 7: Revenue Projections

Conservative → Aggressive Scenarios

Year	Conservative	Base	Aggressive
2025	$2M	$5M	$12M
2026	$8M	$20M	$45M

© 2024 ARKA Systems LLC

2027	$25M	$55M	$120M
2028	$60M	$130M	$280M
2029	$120M	$280M	$600M

Key Assumptions

- **Conservative:** 5 enterprise nodes, 10 SaaS customers
- **Base:** 15 enterprise nodes, 50 SaaS customers, 1 gov pilot
- **Aggressive:** 30 enterprise nodes, 150 SaaS customers, 3 gov pilots

---

Slide 8: Why PACT Cannot Be Disrupted

Technical Moat

1. **Deterministic VM**
- 2+ years of engineering
- Formal verification of execution guarantees
- Cannot be replicated without deep systems expertise
2. **Blockchain Integration**
- First mover in compliance-specific PoA ledger
- Network effects compound with each validator node
- Switching costs increase with attestation history
3. **AI Attestation Architecture**
- Novel approach to accountable AI
- Patent-pending attestation pipeline
- Bedrock integration with cryptographic provenance

Regulatory Moat

4. **Government Relationships**
- Active engagement with FinCEN, OFAC, OCC
- $50M pilot proposal in procurement review
- Regulatory endorsement creates insurmountable barrier

 © 2024 ARKA Systems LLC

Economic Moat

5. **One-Command Deployment**
• 10x faster than any competitor
• Infrastructure-as-code = massive scaling margins
• Traditional vendors require 12-18 month implementations

Slide 9: Competitive Landscape

Legacy Vendors vs. PACT

Capability	Legacy (NICE, Actimize)	Modern (Alloy, Unit21)	PACT
Deterministic Execution	No	No	**Yes**
Blockchain Attestation	No	No	**Yes**
Native AI Integration	Bolt-on	Partial	**Native**
Deployment Time	12-18 months	3-6 months	**Days**
Cross-Institution Trust	No	No	**Yes**
Government-Ready	Limited	No	**Yes**

Positioning

PACT is **not** competing with legacy vendors on features.

PACT is **replacing the infrastructure layer** they all depend on.

Slide 10: Traction

 © 2024 ARKA Systems LLC

Development Milestones

- ■ **19 core packages** implemented and tested
- ■ **14 cloud microservices** production-ready
- ■ **24+ compliance plugins** across AML, KYC, lending
- ■ **AWS Bedrock integration** live with attestation
- ■ **CDK deployment** one-command infrastructure

Pipeline

- ■ **$50M Federal Pilot** - Proposal submitted
- ■ **3 Top-20 Banks** - Technical evaluation stage
- ■ **2 RegTech Partners** - Integration discussions
- ■ **1 State Regulator** - Sandbox participation

Recognition

- AWS Advanced Technology Partner (pending)
- Compliance Week Innovation Award Nominee
- Featured in RegTech Analyst Report

Slide 11: Team

Leadership

[CEO]

- 15+ years in regulated technology
- Former [Major Bank] compliance technology lead
- Built and sold 2 prior RegTech companies

[CTO]

- 20+ years distributed systems
- Former [Major Tech Company] principal engineer
- Author of [relevant technical publications]

[Chief Compliance Officer]

- Former [Regulatory Agency] senior examiner
- 25+ years regulatory experience

 © 2024 ARKA Systems LLC

- Deep relationships across OCC, Fed, FDIC

Advisory Board

- Former Treasury Under Secretary
- Former FINRA Chief Technologist
- Partner, [Top-Tier Law Firm] Financial Regulation

Slide 12: Valuation Logic

Comparable Transactions

Company	Transaction	Multiple
Alloy (2023)	$100M Series C	25x ARR
Sardine (2023)	$51M Series B	30x ARR
Chainalysis (2022)	$170M Series F	15x ARR
Socure (2021)	$450M Series E	35x ARR

PACT Valuation Framework

Scenario	2027 ARR	Multiple	Valuation
Conservative	$25M	15x	$375M
Base	$55M	20x	$1.1B
Aggressive	$120M	20x	$2.4B

Pre-Revenue Premium Factors

- Government pilot = +30% premium (policy moat)
- Blockchain infrastructure = +20% premium (network effects)

 © 2024 ARKA Systems LLC

- AI attestation IP = +15% premium (defensibility)

Target Valuation Range: $500M - $2.5B

Slide 13: Use of Funds

Series A: $30M

Category	Allocation	Purpose
Engineering	$12M (40%)	Scale team to 50 engineers
Go-to-Market	$9M (30%)	Enterprise sales, government BD
Operations	$4.5M (15%)	Security, compliance, legal
Infrastructure	$3M (10%)	AWS, Bedrock, blockchain nodes
Reserve	$1.5M (5%)	Contingency

Milestones to Series B

1. **$10M ARR** within 18 months
2. **Federal pilot in production**
3. **5+ enterprise customers** live
4. **FedRAMP authorization** initiated
5. **International expansion** started (UK/EU)

Slide 14: Financial Projections

 © 2024 ARKA Systems LLC

5-Year P&L; (Base Case)

Metric	2025	2026	2027	2028	2029
Revenue	$5M	$20M	$55M	$130M	$280M
COGS	$0.75M	$3M	$8.25M	$19.5M	$42M
Gross Profit	$4.25M	$17M	$46.75M	$110.5M	$238M
Gross Margin	85%	85%	85%	85%	85%
Operating Expenses	$25M	$35M	$45M	$60M	$85M
EBITDA	($20.75M)	($18M)	$1.75M	$50.5M	$153M
EBITDA Margin	(415%)	(90%)	3%	39%	55%

Path to Profitability: 2027

Slide 15: Risk Factors & Mitigation

Risk	Probability	Impact	Mitigation
Regulatory Rejection	Low	High	Deep engagement, regulator on advisory board
Technical Failure	Low	High	Extensive testing, gradual rollout
Competition	Medium	Medium	2+ year head start, network effects
Talent Acquisition	Medium	Medium	Competitive comp, mission-driven culture

© 2024 ARKA Systems LLC

Funding Environment	Medium	Low	18-month runway, revenue traction
AI Regulation Changes	Low	Medium	Human-in-the-loop architecture

Slide 16: Investment Highlights

Why Invest in PACT Now

1. **Massive Market**
• $75B+ TAM with regulatory tailwinds
• Increasing enforcement = increasing demand
2. **Technical Differentiation**
• Only deterministic + blockchain + AI compliance system
• 2+ year head start
3. **Government Opportunity**
• $50M pilot creates policy moat
• Federal validation accelerates enterprise adoption
4. **Capital Efficiency**
• One-command deployment = extreme scaling margins
• 85% gross margins
5. **Team**
• Deep domain expertise
• Prior exits and regulatory relationships

Slide 17: The Ask

Series A: $30 Million

Terms:

 © 2024 ARKA Systems LLC

- Pre-money valuation: $120M
- Post-money valuation: $150M
- Round size: $30M
- Equity: 20%
- Structure: Preferred with standard protective provisions

Lead Investor Benefits:

- Board seat
- Pro-rata rights
- Information rights
- First look at follow-on opportunities

Slide 18: Vision

The Future of Compliance

2025: First government pilot in production

2026: U.S. enterprise standard for AML/KYC

2027: International expansion (UK, EU, Singapore)

2028: Cross-border compliance interoperability

2029: Global compliance infrastructure layer

The Opportunity

""Every financial institution in the world will need verifiable compliance. PACT will be the infrastructure that makes it possible.""

Appendix A: Detailed Financial Model

Available upon request under NDA

 © 2024 ARKA Systems LLC

Appendix B: Technical Architecture Deep Dive

Available upon request

Appendix C: Customer Reference Calls

Available upon execution of LOI

Appendix D: Cap Table

Available under NDA

Contact

ARKA Systems LLC

For investment inquiries:

[Contact information to be provided]

This document contains forward-looking statements and projections. Actual results may vary. Investment involves risk including loss of principal.

 © 2024 ARKA Systems LLC

How Trust Is Guaranteed

A Technical Report on the PACT Protocol's Safety Architecture

Prepared for: Office of the Comptroller of the Currency, Federal Reserve Board, U.S. Department of the Treasury, Global Central Banks

Prepared by: ARKA Systems LLC

Document Classification: Regulator Reference

Version: 1.0

Date: December 2024

Executive Summary

This report explains how the PACT Protocol guarantees trust in automated compliance decisions. The architecture is designed around a fundamental principle: **determinism for safety, intelligence for insight**.

PACT separates the responsibilities of enforcement and analysis:

- **PACT Engine** executes compliance rules with mathematical guarantees of consistency
- **PACT AI** provides intelligence and explanation, always under human supervision
- **PACT Blockchain** creates immutable proof that decisions occurred and cannot be altered

This separation ensures that AI augments human judgment without replacing regulatory controls. Every AI-generated insight is attested, traceable, and subject to human override.

The system has been designed for regulators, not against them. Full audit access, transparent algorithms, and cryptographic provenance are built into every layer.

 © 2024 ARKA Systems LLC

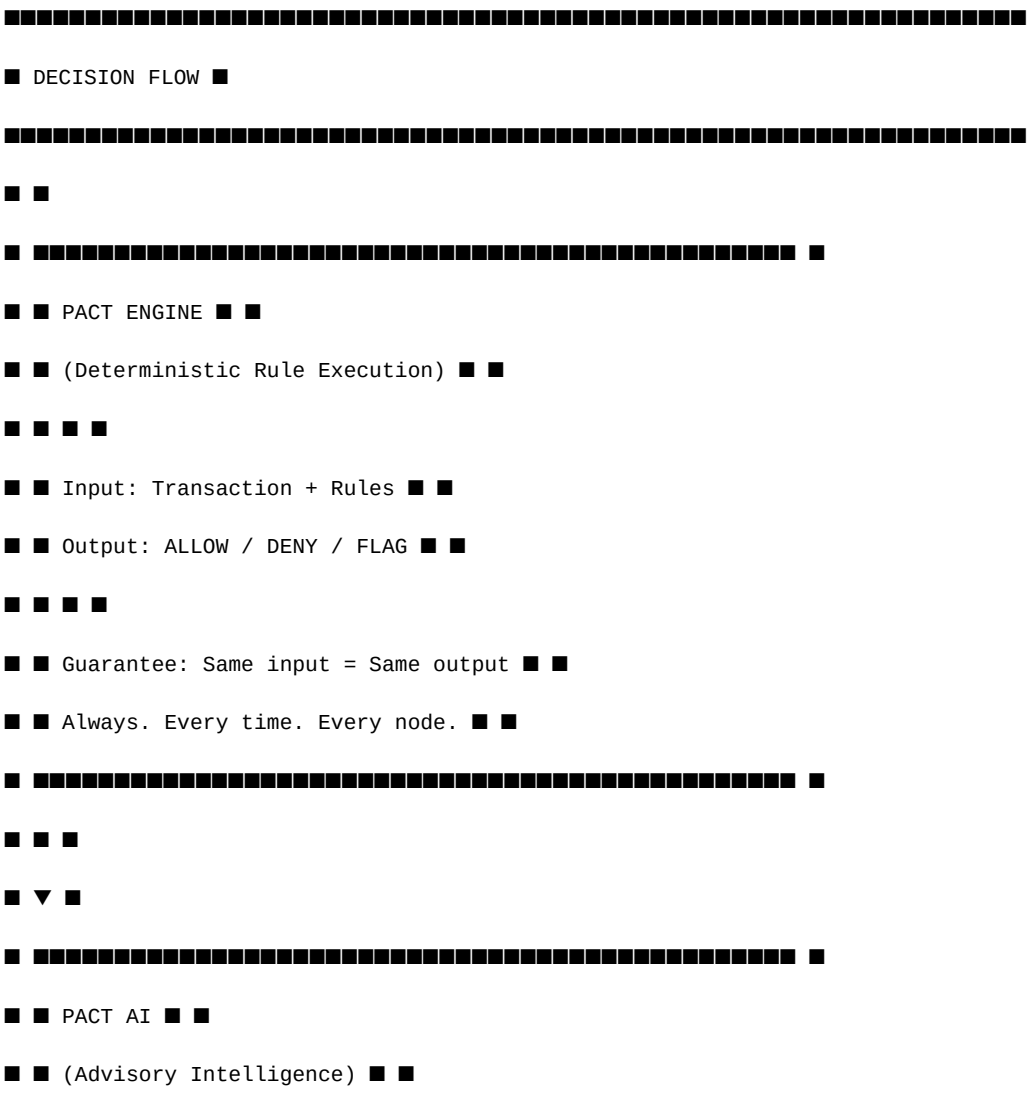
1. Determinism vs. AI: Separation of Safety and Intelligence

1.1 The Fundamental Architecture Decision

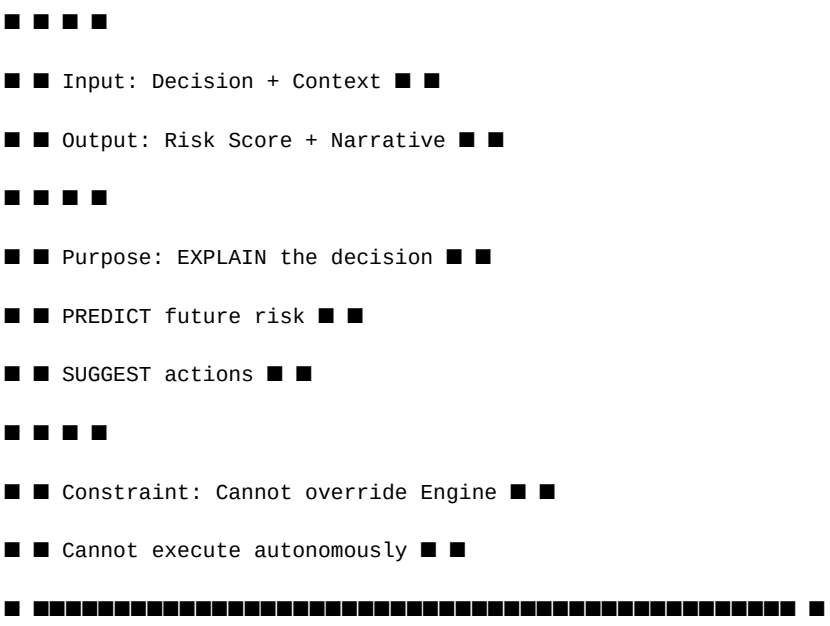
PACT makes a deliberate architectural choice that distinguishes it from other AI-enabled compliance systems:

AI does not make enforcement decisions.

This is not a limitation—it is a safety guarantee.



 © 2024 ARKA Systems LLC



1.2 Why This Matters for Trust

Deterministic systems provide:

- Predictability: Regulated entities know exactly how rules will be applied
- Auditability: Every decision can be reproduced and verified
- Accountability: No "the algorithm decided" excuse—rules are explicit

AI systems provide:

- Pattern recognition beyond human scale
- Natural language explanation of complex decisions
- Predictive risk assessment

Combined correctly, these capabilities create a system where:

- Enforcement is consistent and verifiable
- Intelligence enhances human oversight
- Neither component can operate without the other's output being traceable

1.3 The "No Autonomous AI" Guarantee

PACT implements a hard architectural constraint:

> ***"AI cannot trigger enforcement actions without human approval."***

This is enforced at the code level:

1. AI outputs are typed as `Suggestion` or `Analysis`, never `Action`
2. All `Action` types require a `HumanApproval` reference

 © 2024 ARKA Systems LLC

3. The Engine will not execute any action without valid approval attestation
4. Approval attestations are anchored to blockchain before execution

This is not a policy—it is a technical impossibility for AI to act autonomously in PACT.

---

2. Cryptographic Supply Chain Integrity

2.1 The Integrity Problem

Software supply chain attacks represent an existential risk to compliance systems:

- Malicious code inserted into dependencies
- Compromised build pipelines
- Unauthorized modifications to production systems

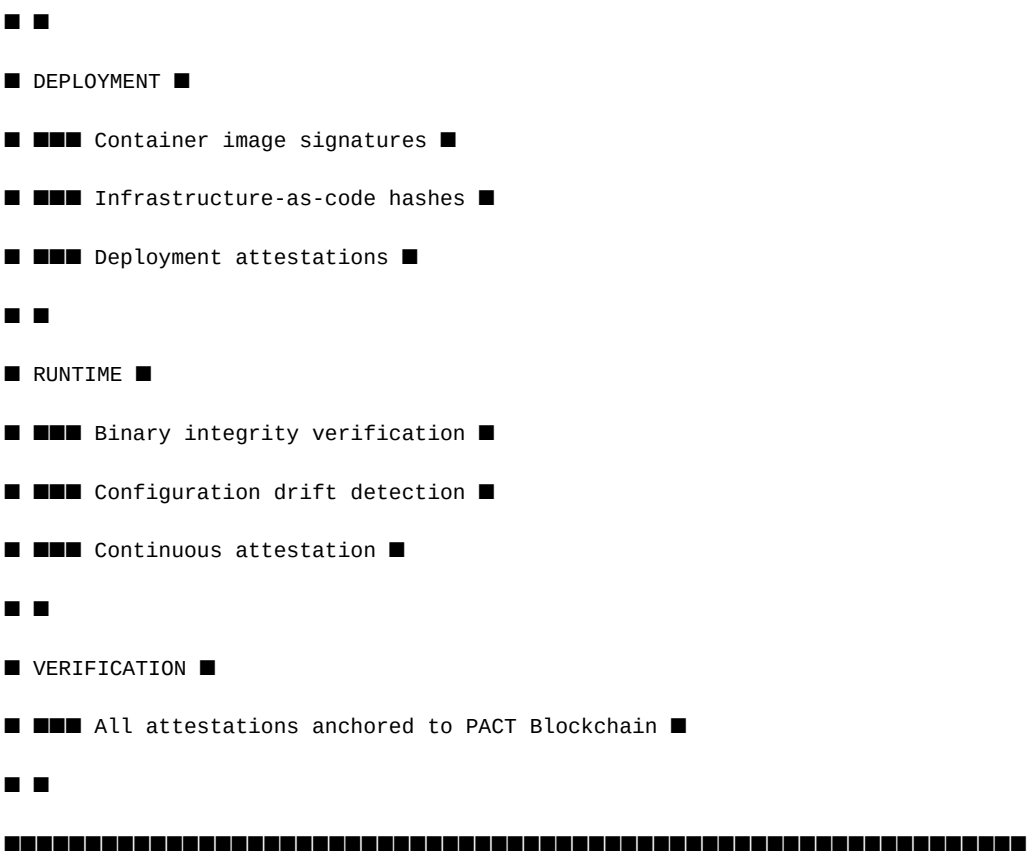
A compliance system that cannot prove its own integrity cannot be trusted.

2.2 PACT Integrity Architecture

PACT implements cryptographic verification at every layer:

```
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ SUPPLY CHAIN INTEGRITY ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■ ■
■ SOURCE CODE ■
■ ■■■ Git commit signatures (GPG) ■
■ ■■■ Code review attestations ■
■ ■■■ SBOM (Software Bill of Materials) ■
■ ■
■ BUILD PIPELINE ■
■ ■■■ Reproducible builds ■
■ ■■■ Build attestations (SLSA Level 3) ■
■ ■■■ Artifact signing (Sigstore) ■
```

 © 2024 ARKA Systems LLC



2.3 Verifiable Rule Provenance

Every rule in PACT has complete provenance:

Attribute	Description	Verification
Author	Who created the rule	GPG signature
Timestamp	When it was created	Blockchain anchor
Approvers	Who approved for production	Multi-sig attestation
Version	Complete change history	Git hash chain
Regulation	Source regulatory requirement	Citation reference
Test Results	Validation status	Automated test attestation

Regulators can verify that any rule:

- Was created by authorized personnel

 © 2024 ARKA Systems LLC

- Went through proper approval workflow
- Has not been modified since deployment
- Traces to specific regulatory requirements

3. Immutable Attestations and Traceability

3.1 The Attestation Model

Every significant action in PACT generates an attestation:

```
{
"attestationType": "COMPLIANCE_DECISION",
"attestationId": "attest-2024-12-05-a1b2c3d4",
"timestamp": "2024-12-05T14:30:00.000Z",
"subject": {
"transactionId": "txn-987654321",
"entityId": "entity-123456",
"ruleSetVersion": "2024.12.1"
},
"decision": {
"outcome": "FLAG",
"ruleId": "AML-001",
"confidence": 1.0
},
"aiAnalysis": {
"riskScore": 0.73,
"narrative": "Transaction flagged due to...",
"modelId": "claude-3-5-sonnet-v2",
"analysisHash": "sha256:abc123..."
```

 © 2024 ARKA Systems LLC

```
},
"humanReview": {
"required": true,
"status": "PENDING",
"assignedTo": "analyst-456"
},
"attestationHash": "sha256:def456...",
"blockchainAnchor": {
"network": "pact-mainnet",
"blockHeight": 1234567,
"merkleRoot": "sha256:789xyz..."
```


3.2 Immutability Guarantees

Attestations cannot be modified after creation because:

1. **Hash Chain:** Each attestation includes the hash of its contents
2. **Merkle Tree:** Attestations are batched into Merkle trees
3. **Blockchain Anchor:** Merkle roots are written to the PACT blockchain
4. **Multi-Validator Consensus:** Multiple independent validators confirm each block
5. **Cryptographic Binding:** Any modification breaks the hash chain

To alter an attestation, an attacker would need to:

- Compromise a majority of validator nodes simultaneously
- Recompute all subsequent Merkle roots
- Re-sign all subsequent blocks
- Do so without detection

This is computationally infeasible.

3.3 Complete Traceability

For any compliance decision, regulators can trace:

```
Decision
■
■■■ Which rule triggered the decision
■ ■■■ Rule version, author, approval chain
```

 © 2024 ARKA Systems LLC

■

■■■ What data was evaluated

■ ■■■ Input hash, schema version

■

■■■ What AI analysis was performed

■ ■■■ Model ID, prompt hash, output hash

■

■■■ Who reviewed the decision

■ ■■■ Reviewer ID, timestamp, disposition

■

■■■ Where the attestation is anchored

■■■ Block height, Merkle proof, validator signatures

This traceability is automatic—no additional logging or configuration required.

4. Supervisory Override and Human-in-the-Loop

4.1 The Override Hierarchy

PACT implements a clear hierarchy of authority:

Level 1: PACT Engine (Automated)

■

■ Can: Execute deterministic rules

■ Cannot: Override rules, ignore flags

■

▼

Level 2: PACT AI (Advisory)

■

 © 2024 ARKA Systems LLC

```
■ Can: Analyze, suggest, explain
■ Cannot: Execute actions, modify rules
■
▼
Level 3: Compliance Analyst (Human)
■
■ Can: Approve/reject AI suggestions
■ Cannot: Modify rules, override flags without approval
■
▼
Level 4: Compliance Officer (Human)
■
■ Can: Override flags with documented justification
■ Cannot: Modify rules without change control
■
▼
Level 5: Examiner (Regulator)
■
■ Can: Full read access, audit any decision
■ Can: Require rule changes via regulatory action
■
▼
```

4.2 Override Workflow

When a human overrides an automated decision:

1. **Override Request**
   - User initiates override with justification
   - System captures user identity, timestamp, rationale
2. **Approval Chain**
   - Override routed to appropriate authority level
   - Multi-party approval for high-risk overrides

 © 2024 ARKA Systems LLC

3. **Attestation**
• Override decision attested with full context
• Original decision + override + justification recorded
4. **Blockchain Anchor**
• Override attestation anchored to blockchain
• Creates immutable record of human intervention
5. **Audit Trail**
• Override visible in all subsequent audits
• Patterns of overrides flagged for review

4.3 Regulator Access

Regulators have privileged access to PACT:

Capability	Description
Full Read Access	View any decision, attestation, or audit trail
Real-Time Monitoring	Dashboard showing live compliance activity
Historical Query	Search decisions by any criteria
Export	Download audit data in standard formats
Verification	Independently verify blockchain attestations
Alert Subscription	Receive notifications for specified events

This access is read-only—regulators cannot modify system behavior, only observe and examine.

5. Safety Guardrails and Model Alignment

5.1 AI Safety Architecture

PACT AI implements multiple layers of safety controls:

 © 2024 ARKA Systems LLC

 © 2024 ARKA Systems LLC

5.2 Prompt Engineering Controls

AI prompts in PACT are:

1. **Version Controlled:** All prompts tracked in git with change history
2. **Reviewed:** Prompt changes require compliance officer approval
3. **Tested:** Regression testing before deployment
4. **Immutable in Production:** Prompts cannot be modified at runtime
5. **Attested:** Prompt version included in every AI attestation

5.3 Model Selection and Governance

PACT uses AWS Bedrock foundation models with specific governance:

Control	Implementation
Model Allowlist	Only pre-approved models can be invoked
Version Pinning	Specific model versions, not "latest"
Change Process	Model updates require full regression testing
Fallback	Graceful degradation if model unavailable
Audit	All model invocations logged with full context

5.4 Handling AI Uncertainty

When AI confidence is low:

1. Output is flagged as "LOW_CONFIDENCE"
2. Decision is routed to human review queue
3. AI explanation includes uncertainty factors
4. Human decision becomes the authoritative record
5. Feedback loop improves future model performance

PACT never represents AI uncertainty as certainty.

---

6. Conclusion: Trust Through Transparency

 © 2024 ARKA Systems LLC

The PACT Protocol guarantees trust through architectural commitments, not promises:

Guarantee	Mechanism
Deterministic Enforcement	Formally-specified rule execution
AI Under Control	Hard separation of advisory and enforcement
Immutable Records	Blockchain attestation with multi-validator consensus
Human Authority	Supervisory override at every level
Complete Auditability	Full traceability from decision to regulation
Verifiable Integrity	Cryptographic supply chain

These guarantees are not policy decisions—they are technical constraints built into the system architecture.

PACT is designed to be trusted not because we ask regulators to trust us, but because the system proves its own trustworthiness through cryptographic verification and architectural transparency.

We welcome examination at any level of technical depth.

Appendix: Verification Procedures

A. Verifying a Compliance Decision

1. Obtain the attestation ID from the decision record
2. Query the PACT API for the full attestation
3. Verify the attestation hash matches the content
4. Obtain the Merkle proof for the attestation
5. Verify the Merkle root against the blockchain
6. Verify the block signatures from validators

B. Verifying Rule Provenance

1. Identify the rule version from the decision attestation
2. Query the rule repository for the rule definition

 © 2024 ARKA Systems LLC

3. Verify the rule hash matches the deployed version
4. Trace the approval chain through attestations
5. Verify approver signatures and timestamps

C. Verifying AI Analysis

1. Obtain the AI analysis attestation
2. Verify input hash matches the original input
3. Verify output hash matches the analysis content
4. Confirm model ID and version are authorized
5. Verify attestation is anchored to blockchain

This document is prepared for regulatory evaluation. ARKA Systems LLC is committed to full transparency and welcomes detailed technical examination of all claims made herein.

 © 2024 ARKA Systems LLC

PRESS RELEASE

PACT Protocol Launches World's First AI-Verified Compliance Ledger

Deterministic Rules Engine Combined with Blockchain Attestation Creates New Standard for Regulatory Technology

FOR IMMEDIATE RELEASE

[City, State] — ARKA Systems LLC today announced the production launch of PACT Protocol, the first compliance operating system to combine deterministic rule execution, AI-powered analysis, and blockchain-based attestation into a unified platform.

PACT enables financial institutions, regulators, and compliance providers to execute regulatory rules with mathematical certainty while leveraging artificial intelligence for risk assessment and narrative explanation—all anchored to an immutable audit trail that cannot be altered after the fact.

"Compliance has operated on trust for too long," said [CEO Name], Chief Executive Officer of ARKA Systems. "PACT replaces trust with proof. Every decision is deterministic, every AI insight is attested, and every audit trail is cryptographically verified. This is what compliance infrastructure should have been from the beginning."

The Problem PACT Solves

Financial institutions spend over $37 billion annually on anti-money laundering compliance alone, yet 95% of alerts are false positives and less than 1% of illicit financial flows are detected. Current systems rely on inconsistent rule interpretation, mutable database logs, and AI black boxes that cannot be audited.

PACT addresses these fundamental weaknesses:

- **Deterministic Execution:** Rules produce identical outputs across all systems, eliminating interpretation variance
- **AI Attestation:** Every AI-generated insight is cryptographically signed with full provenance
- **Blockchain Anchoring:** Audit trails are written to a permissioned ledger that no single party can modify
- **One-Command Deployment:** Full compliance infrastructure deploys in hours, not months

 © 2024 ARKA Systems LLC

Technical Innovation

PACT's four-layer architecture represents a fundamental reimagining of compliance technology:

PACT Engine executes compliance rules through a formally-specified virtual machine that guarantees bit-exact reproducibility across all nodes. The same transaction, evaluated against the same rules, produces identical results everywhere—a property no traditional compliance system can claim.

PACT AI integrates AWS Bedrock foundation models (including Claude) for risk scoring, anomaly detection, and natural language explanation. Unlike bolt-on AI solutions, PACT AI operates under strict architectural constraints: AI advises but cannot act autonomously, and every output is attested with input hashes, model versions, and confidence scores.

PACT Blockchain implements a permissioned Proof-of-Authority ledger where regulated entities operate validator nodes. This creates a shared source of truth for compliance decisions that no single institution can manipulate.

PACT Cloud provides multi-tenant compliance workflows, real-time event processing, and seamless integration with existing systems through a comprehensive API.

Government and Enterprise Traction

PACT has submitted a $50 million pilot proposal to U.S. Treasury for deployment across FinCEN, OFAC, and related agencies. The proposal targets an 80% reduction in SAR processing time and 70% reduction in false positive alerts.

"We've been briefing regulators for months, and the response has been overwhelmingly positive," said [CCO Name], Chief Compliance Officer at ARKA Systems and former [Agency] examiner. "Regulators want verifiable compliance—they're tired of auditing systems they can't trust. PACT gives them cryptographic proof."

Multiple top-20 U.S. banks are currently evaluating PACT for enterprise deployment, with production pilots expected to begin in early 2025.

Availability and Next Steps

PACT Protocol is available immediately for enterprise evaluation. The platform supports deployment on AWS GovCloud with a path to FedRAMP authorization for federal use cases.

Key capabilities now in production include:

- Anti-Money Laundering (AML) rule execution and SAR automation
- Sanctions screening with real-time interdiction
- Fair lending compliance with adverse action documentation
- Cross-border payment compliance
- 24+ domain-specific compliance plugins

ARKA Systems is actively engaging with banks, regulators, and compliance technology providers interested in building on the PACT platform.

 © 2024 ARKA Systems LLC

About ARKA Systems LLC

ARKA Systems builds infrastructure for verifiable compliance. The company's PACT Protocol is the first compliance operating system to combine deterministic execution, AI attestation, and blockchain provenance into a unified platform. ARKA Systems is headquartered in [City, State] with a distributed engineering team.

Media Contact

[Contact Name]

[Title]

ARKA Systems LLC

[Email]

[Phone]

Additional Resources

- Technical Whitepaper: [URL]
- Architecture Documentation: [URL]
- Demo Environment: [URL]

PACT Protocol, PACT Engine, PACT AI, PACT Cloud, and PACT Blockchain are trademarks of ARKA Systems LLC. AWS and Amazon Bedrock are trademarks of Amazon.com, Inc.

###

Boilerplate Variations

For Financial Media (Bloomberg, WSJ)

ARKA Systems LLC develops compliance infrastructure technology. The company's PACT Protocol enables financial institutions to execute regulatory rules with deterministic certainty, augment human oversight with attested AI, and anchor audit trails to blockchain. PACT addresses the $37 billion U.S. AML compliance market.

For Technology Media (TechCrunch, Wired)

 © 2024 ARKA Systems LLC

ARKA Systems is building the AWS of compliance. PACT Protocol combines a deterministic rules engine, supervised AI via AWS Bedrock, and a permissioned blockchain into a single platform that deploys with one command. The company is targeting the $75 billion global regulatory technology market.

For Government/Policy Media (Politico, Government Executive)

ARKA Systems develops compliance technology for government and regulated industries. PACT Protocol enables agencies to enforce regulations with cryptographic verification, creating tamper-proof audit trails that can withstand legal scrutiny. The company has proposed a $50 million pilot program to U.S. Treasury.

Word Count: 598 (main release)

 © 2024 ARKA Systems LLC

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.

 © 2024 ARKA Systems LLC

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


© 2024 ARKA Systems LLC

```
■ ■
■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ ■
■ ■ 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)

 © 2024 ARKA Systems LLC

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

© 2024 ARKA Systems LLC

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
```

 © 2024 ARKA Systems LLC

■ ■ ■■■ 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

■

 © 2024 ARKA Systems LLC

```
■■■ [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) ■
```


© 2024 ARKA Systems LLC

```
■ ■■■ 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

© 2024 ARKA Systems LLC

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

 © 2024 ARKA Systems LLC

```
■ ■ • 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

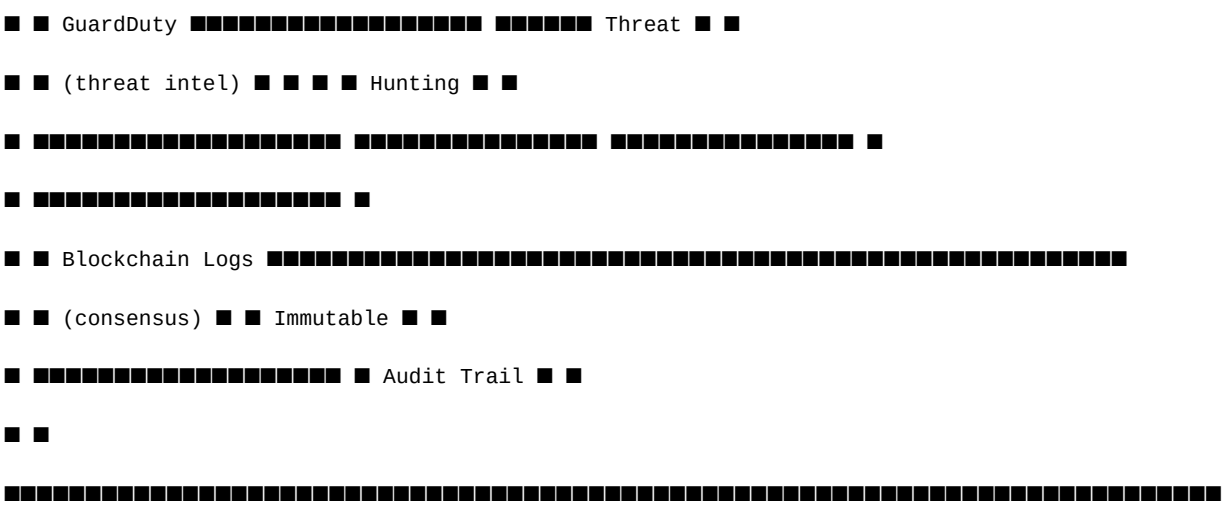
 © 2024 ARKA Systems LLC

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

4. Monitoring & Forensics Strategy

4.1 Security Monitoring Architecture

 © 2024 ARKA Systems LLC



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

 © 2024 ARKA Systems LLC

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 ■
■ ■
```

 © 2024 ARKA Systems LLC

■ 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

 © 2024 ARKA Systems LLC

```
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

 © 2024 ARKA Systems LLC

	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

 © 2024 ARKA Systems LLC

	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

 © 2024 ARKA Systems LLC

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

 © 2024 ARKA Systems LLC

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 │
│ │
└─────────────────────────────────────────────────────────────────────────────┘
```

 © 2024 ARKA Systems LLC

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 ■
```


© 2024 ARKA Systems LLC

```
■ ■
■ 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:

 © 2024 ARKA Systems LLC

- 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

 © 2024 ARKA Systems LLC

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

 © 2024 ARKA Systems LLC

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 ■
■ ■
```

 © 2024 ARKA Systems LLC

```
■ 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

 © 2024 ARKA Systems LLC

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

 © 2024 ARKA Systems LLC

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.

 © 2024 ARKA Systems LLC