Stratosphere Audit Packet (Procurement & Security Review)

Overview

This audit packet provides procurement and security teams with a concise overview of Stratosphere's Compliance Toolkit (PACT), including security architecture, compliance alignment, and cryptographic integrity model designed to support SOC 2 Type II and HIPAA-aligned environments.

Security Model

Stratosphere implements a cryptographic integrity layer that ensures system events are hashed, chained, and independently verifiable. This provides tamper-evident audit trails and reduces reliance on implicit trust in internal systems.

Compliance Alignment

PACT is designed to support SOC 2 Trust Services Criteria (Security, Availability, Confidentiality, Processing Integrity) and HIPAA Security Rule requirements. It strengthens audit evidence generation but does not certify compliance.

SOC 2 Control Mapping Summary

Category	PACT Capability
Security (CC6/CC7)	Access logging + cryptographic event tracking
Availability (CC7)	Operational event monitoring and logging
Processing Integrity	Sequential hashing + tamper detection
Confidentiality	Encrypted workflows + access-scoped logging
Change Management (CC8)	Verifiable system change events

Audit Evidence Model

System events are captured, hashed using SHA-256, and chained into an immutable sequence. This enables independent verification of integrity and detection of any tampering or alteration of historical records.

Important Notice

Stratosphere does not certify SOC 2 compliance or HIPAA compliance. Customers remain responsible for their own compliance programs and control environment implementation.