ALIANZA

Platform Audits

Gain detailed health, performance, and security insights into your environments within the Alianza Core platform with three different audit types.

Platform issues rarely announce themselves. Capacity ceilings, configuration drift, and unpatched vulnerabilities accumulate quietly—until they affect service delivery or force reactive, unplanned work. Available standalone, or through Alianza's professional services solution Expert Services, platform audits are designed to surface these risks before they reach that point.

Three audit types are available—Capacity, Network, and Security—each conducted by a PS Engineer with direct access to the service provider's environment. No data compilation required, no external handover, no gaps from working with secondhand information. Each audit delivers a written findings report covering identified risks, severity classification where applicable, and prioritized remediation recommendations.

Audits are available as add-ons for Technical Retainer and Strategic Partnership packages. Embedded Advisor includes one annual audit of the service provider's choice, conducted outside of the quarterly hour allocation. Service providers without an Expert Services retainer can also purchase any audit type as a standalone engagement through the standard PS statement of work (SOW) process.

Capacity Audit

Knowing what the Core platform is doing today is the foundation for every infrastructure decision made tomorrow. A capacity audit delivers a point-in-time view of how a Core environment is being utilized:

- **License Usage.** Consumed vs. available license capacity across the platform.
- **Performance and Platform Load.** System load against recommended thresholds.
- **Feature Usage.** Utilization of key capabilities including Class 5 capabilities, transcoding , and dual-tone multi-frequency (DTMF) signaling.

Findings are delivered in a utilization report that identifies risks and recommends actions. **The result is a clear, evidence-based picture of where your platform stands**—surfacing over-provisioning that may be driving unnecessary cost, under-provisioning that could affect service quality, and the data needed to plan confidently for growth, contract renewals, or migration decisions before capacity becomes a problem.

Most Valuable for

- **Contract renewal** and commercial planning, to strategize from a position of data instead of relying on assumptions.
- **Growth initiatives** where upcoming customer expansion, market growth, or major onboarding initiative requires confidence that the platform can scale to meet demand.
- **Performance optimization** where unexplained platform slowdowns or stability concerns warrant a structured assessment to identify capacity constraints and improvement opportunities.

Network Audit

A network that looks stable today may carry hidden risk in the configurations and design decisions made years ago.
Most network problems don't appear out of nowhere. Certificates expire on a known schedule. Configurations drift when changes accumulate over time. Routing logic that worked at one scale starts creating edge cases at another.

The network audit finds these before an end users does—reviewing Core architecture, configuration health, and routing logic of deployed environments against current best practices to deliver a prioritized remediation report that tells your teams exactly what to address and in what order.

- **Active Alarm Review.** Critical and Major alarms that go unresolved long enough tend to disappear into the background, until they don't. Surface active alarms, what each means, and clear resolution guidance that service providers can act on directly.
- **Network Design.** Access and trunking architecture analysis to identify structural gaps and design deviations.
- **Hardware and Layout.** Physical and logical layout evaluation or confirmation that virtualized infrastructure adheres to current best practices.
- **Connectivity & Routing.** Validate network peerings, routing relationships, and redundancy to identify misconfigurations and potential points of failure.
- **Certificate Health.** Review TLS certificates for validity, expiration dates, encryption standards, and configuration to maintain secure communications.

- **DNS Configuration.** Assess DNS, SIP domain, and related configurations to ensure reliable service routing, resilience, and security. DNS misconfigurations—particularly in environments with multiple Session Border Controllers (SBCs) or geo-redundant core deployments—are among the most error-prone configuration areas and often go undetected until an outage exposes that expected resiliency did not hold. Validate that public DNS resolves correctly, and that core routing domains are configured in line with the intended design.
- **Configuration Health.** Identification of outdated configurations and deviations from recommended standards.
- **Translations and Routing.** Review dial plan logic, routing rules, and translation accuracy— including configuration efficiency that identifies the patterns before complexity becomes a liability. Routing that works well on a small scale may accumulate redundant or duplicated elements over time, making it difficult to manage as the environment grows.

Findings are delivered in a report covering configuration issues, design observations, and prioritized remediation recommendations. The result is a clear, actionable strategy for closing gaps before they become outages—giving service providers the confidence that their network is built to support current demand and resilient enough to handle what comes next.

Most Valuable For

- **Configuration creep** and incremental modifications as the environments have evolved over time, where documentation has not kept pace, and no one has taken a full inventory of whether what is running today still reflects best practices.
- **Milestone preparation** for an upgrade or migration when a clear, authoritative picture of their current network state is needed before introducing additional complexity.
- **Troubleshooting recurring issues** like unexplained call quality problems, routing anomalies, or intermittent failures that have not been fully resolved and may have architectural roots.

ALIANZA

Security Audit

A security gap that goes undetected is a liability that cannot be managed.

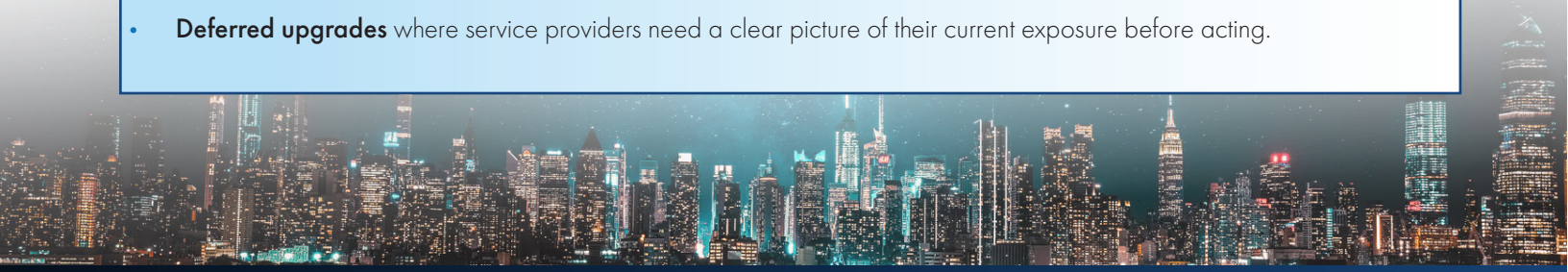
Not every service provider has a dedicated resource monitoring platform security, and published advisories only create value if there is a team member able to act on them. Confirm the Core platform's exposure:

- **Vulnerability Assessment.** Environment review against published Alianza Security Alerts and Critical Security Advisories to identify known exposure points.
- **Active Alarm.** Identification of unresolved alarms with direct or indirect security implications.
- **Software Version.** Flagging of components running outdated or end-of-support versions that represent unpatched risk.

Findings are delivered in a report covering identified vulnerabilities, severity classification, and recommended remediation steps.

Most Valuable For

- **Lean teams** who cannot realistically monitor every advisory and product alert and would benefit from a trusted expert to assess relevance, filter out the noise, and highlight the actions that deserve immediate attention.
- **Regulated environments** where a documented, third-party, evidence-based assessment is needed to demonstrate due diligence.
- **Deferred upgrades** where service providers need a clear picture of their current exposure before acting.



Alianza delivers full-stack, cloud-native communications network services with carrier-grade infrastructure and support to advance network modernization for service providers.

The Alianza Intelligent Communications Fabric empowers service providers to lead in the emerging era of AI-driven voice networks and services. By bridging legacy systems with modern software-defined technologies, we enable providers to simplify operations, innovate faster, and monetize new opportunities in business and consumer voice.