Checklist for Migrating to Cloud-Native Call Handling

Assessing Infrastructure Readiness

Network Capacity: Check if your network infrastructure (either vendor-provided or self-provided) can handle increased data traffic, including real-time video for up to 30% of call volume, location data for up to 95% of call volume, and other multimedia content for 20% of call volume.

Intra, Inter, and External Connectivity: Review connectivity that currently exists within your buildings, between your buildings, and to external sources such as manager service providers to support your migration.

Fault-Tolerant Design: Verify that your infrastructure supports redundancy and fault tolerance, minimizing service interruptions during hardware failures, to realize 5-nines (99.999%) availability - in other words, 5 minutes of downtime a year.

Security Enhancements

Secured Audio and Video Delivery: Implement password protection, domain-level security, and link-sharing protection to safeguard multimedia content.

Data Classification: Categorize data based on sensitivity and apply appropriate security measures, balancing strict security with operational flexibility.

Data Protection: Utilize robust network security controls, proactive security measures, government-grade cloud storage, and data protection solutions to secure data at rest and in transit.

More Details ➔

System Scalability and Performance

Scalability: Confirm that the NG911 solution can scale to meet future demands, including handling 50% higher call volumes and supporting 25% additional users.

Performance Monitoring: Implement 24x7x365 automated monitoring systems to detect unusual activities, monitor server performance, and support network availability.

Minimizing Disruptions: Verify that your vendor would minimize disruptions to your systems during updates and upgrades, so that you can achieve the agreed Service Level Agreement (SLA) promised by the vendor.

Authentication, Authorization, and Accounting (AAA)

Authentication and Authorization: Utilize industry-standard protocols like OAuth 2.0 for secure user authentication and access control.

Role-Based Access Control (RBAC): Define user roles and permissions based on job functions, providing appropriate access levels for all users.

Multi-Factor Authentication (MFA): Implement MFA to add an extra layer of security for user accounts.

Data Management and Storage

Securing Data at Rest and in Transit: Encrypt data both at rest and during transmission to prevent unauthorized access.

Key Management: Use centralized key management services for encryption, and institute regular key rotation for enhanced security.

Database Security: Verify that database systems are isolated, encrypted, and capable of scaling to meet your storage needs.

More Details ➔

Compliance and Auditing

Regular Auditing: Set up a regular schedule for reviewing user access and system performance, to be in compliance with security policies.

Logging and Monitoring: Implement extensive logging of operational metrics and set alarms for threshold breaches, enabling rapid response to potential issues.

Disaster Recovery and Business Continuity

Redundancy: Verify that your NG911 system has a robust disaster recovery plan, including data replication and failover mechanisms.

Environmental Safety: Verify that your data centers are equipped with fire detection, climate control, and redundant power supplies to prevent outages.

More Details ➔

Physical and Internal Security

Physical Security: Protect data centers and offices with 24x7 alarm systems and secure access controls.

Internal Security Policies: Implement two-factor authentication and secure VPNs for remote access, and regularly update security measures.

Training and Support

User Training: Provide comprehensive training (instructor-led as well as online on-demand) for PSAP personnel on the new system, focusing on security practices, system features, and troubleshooting.

Supervisor Training: Check that adequate training (instructor-led as well as online on-demand) is provided for management staff, and consider how your protocols may evolve, for example when you start receiving video-to-911 calls for the first time.

Support Services: Verify access to 24x7 support from your NG911 provider, with clear escalation procedures for critical issues.

For a free demonstration of the benefits your center can expect from migrating to cloud-native call handling solutions, please visit https://carbyne.com/request-a-demo/

CARBYNE

With Carbyne, Every Person Counts

OFFICES IN:

USA | ISRAEL | MEXICO

For more information or to schedule a demo, visit **carbyne.com**