

Critical Insights

FREE RESOURCE · PUBLIC SAFETY MISSION-CRITICAL COMMUNICATIONS

MCX Migration Readiness Checklist

Preparing to move from TETRA or P25 to LTE/5G mission-critical broadband

Use this checklist to pressure-test your organisation's readiness *before* the network is built. It gathers the questions that, left until "later", tend to become the crises of an MCX programme — drawn from 25+ years supporting emergency services and critical-communications programmes worldwide.

1 · Strategy & governance

- ☐ A clear statement of the operational outcomes migration must deliver (not just "replace TETRA")
- ☐ Named senior owner accountable for the capability, not only the technology
- ☐ Realistic timeline with parallel-running / dual-carriage period defined
- ☐ Business case tested against the "bad day", not just the demo

2 · Coverage & capacity

- ☐ Coverage parity mapped against today's TETRA/P25 footprint — including tunnels, basements, rural edge and in-building
- ☐ Special-event and surge capacity understood at the busiest cells
- ☐ Approach agreed for coverage gaps (deployables, in-building systems, satellite/NTN)
- ☐ Independent verification of vendor coverage claims planned

3 · Scalability & large groups ("XL Groups")

- ☐ Maximum group sizes for all-informed situational awareness quantified — hundreds of users routinely, and thousands in major incidents or public-order operations
- ☐ The way the solution *assembles* large group calls understood — members joined to the call on affiliation, versus invited at the instant push-to-talk is pressed
- ☐ "Near-instant" (sub-300 ms) group-call set-up *evidenced at the largest required group sizes* — not just at proof-of-concept or plug-test scale
- ☐ Per-member signalling growth tested (SIP INVITE / Connect Request load rising in direct proportion to group size)
- ☐ Late-entry behaviour proven for members out of coverage when the call begins
- ☐ Performance validated under concentrated load (a large group within a single cell)
- ☐ XL Group performance written into acceptance criteria and independently verified in the field, not asserted

4 · Devices, accessories & applications

- ☐ Devices certified for the operational environment (rugged, intrinsically safe where needed)
- ☐ Push-to-talk accessories tested with gloves, in the wet, across a full shift
- ☐ Battery life validated against real duty cycles
- ☐ Applications match frontline muscle memory under stress

5 · Control room & interfaces

- ☐ Dispatch / ICCS integration scoped and tested end-to-end

- ☐ Talkgroup and fleet-map design reviewed with real users
- ☐ Interworking with legacy TETRA/P25 during transition proven
- ☐ Logging, recording and replay requirements met

6 • Resilience & fallback

- ☐ Graceful degradation behaviour understood and acceptable
- ☐ Credible fallback for commercial-network outage
- ☐ Prioritisation, pre-emption and QoS (MCPTT) validated under load
- ☐ Power, transmission and core redundancy assured

7 • Cybersecurity, data protection & evidential integrity

- ☐ End-to-end security and encryption model agreed — for voice *and* for data at rest and in transit
- ☐ Security of data captured by MCX apps on smartphones — images, video, messages (MCData) and documents — addressed at app, device and server/cloud layers (an area most MCX solutions have barely considered)
- ☐ Evidential integrity of captured media — a defined master copy, tamper-evidence and a full audit trail of any editing or processing (per ACPO/NPIA *Practice Advice on Police Use of Digital Images* and the Digital Imaging Procedure — cited as a requirement in recent national bids)
- ☐ Chain of continuity & disclosure — media retrievable and producible for court in an unaltered, admissible form, with full disclosure schedules (Article 6 ECHR: right to a fair trial)
- ☐ Secure storage, retention & disposal — where evidential data resides (device, MCX core, cloud), data sovereignty / jurisdiction, and retention/deletion to legislative time limits
- ☐ Access control, key management & logging — who can view, export or delete captured evidential data, and a record of who did
- ☐ Mobile device & app-data protection — MDM, containerisation of MCX app data, remote wipe on loss or theft; BYOD risks addressed
- ☐ Data-protection compliance (UK GDPR / DPA 2018) and vendor security posture evidenced — penetration testing, accreditation (e.g. ISO 27001, NCSC principles), supply-chain assurance and 3GPP MCX security conformance — evidenced, not asserted

8 • Users, training & change

- ☐ Frontline users engaged from the start, not at go-live
- ☐ Training and adoption plan resourced as a work-stream
- ☐ Confidence-building trials in real operational conditions
- ☐ Clear, honest communication on what changes and what doesn't

9 • Commercial & transition

- ☐ Contract holds suppliers to operational outcomes, not just delivery milestones
- ☐ Exit, portability and lock-in risks understood
- ☐ Zero-downtime transition plan for business-as-usual
- ☐ Independent bid / delivery assurance in place

Where Critical Insights helps

We provide independent, technically-grounded support across every item above — from board advisory and migration planning to coverage, XL-Group scalability, cybersecurity and evidential-data assurance, bid support and programme recovery. If any line on this checklist is a worry, let's talk.

www.criticalinsights.net · info@criticalinsights.net · +44 20 7861 4429