

# Towner's Mitel Readiness & Risk Assessment

This document is designed to help organizations evaluate the *operational readiness, risk exposure, and long-term viability* of an existing or planned Mitel communications environment. It is not a sales tool. It is intended to support informed decision-making by IT leadership, operations teams, and executive stakeholders.

*This framework reflects how enterprise communications platforms are evaluated internally at scale – balancing lifecycle, risk, and operational continuity.* This framework reflects how Mitel environments are evaluated internally at the vendor level and by experienced operators in production environments.

## How to Use This Assessment

- This document should be completed collaboratively by IT, operations, and business leadership.
- Not all sections will carry equal weight for every organization.
- Areas marked **High Risk** do not imply failure. They indicate where deeper planning or mitigation is required.



## 1. Platform & Version Awareness

**Objective:** Establish clarity on what is actually deployed and supported.

- Primary Mitel platforms in use (MiVoice Business, MiCollab, Mitel Connect, etc.)
- Software versions deployed by location
- Hardware models and quantities
- License types and entitlements verified
- Support status confirmed (active, extended, approaching retirement)

**Risk Indicators:** - Version inconsistency across sites - Unsupported or undocumented hardware - Unknown licensing status

## 2. Lifecycle & Support Exposure

**Objective:** Understand real lifecycle risk versus perceived urgency.

- Vendor support timelines documented
- Extended support dependencies identified
- Internal tolerance for maintenance-only platforms defined
- Replacement timelines (if any) aligned to business cycles

**Risk Indicators:** - Decisions driven by fear rather than timelines. No internal ownership of planning lifecycle

### 3. Operational Reliability & Survivability

**Objective:** Ensure communications continuity under adverse conditions.

- Local call processing requirements defined
- WAN outage behavior documented
- Power redundancy validated by site
- Emergency calling behavior verified

**Risk Indicators:** - Assumptions about cloud availability - Lack of survivability testing

### 4. Network & Infrastructure Dependencies

**Objective:** Identify dependencies that affect voice quality and availability.

- Network readiness for real-time voice confirmed
- QoS policies documented and enforced
- SIP trunk dependencies mapped
- Firewall and security policies reviewed

**Risk Indicators:** - Voice competing with best-effort traffic - Undocumented third-party dependencies

### 5. Integration & Application Dependencies

**Objective:** Understand how Mitel fits into the broader application ecosystem.

- Microsoft Teams or other collaboration platforms identified
- CRM, contact center, and paging integrations documented
- API or middleware dependencies known

**Risk Indicators:** - One-way integrations - Unsupported third-party tools

### 6. Organizational Readiness

**Objective:** Align technology decisions with people and process realities.

- Internal support ownership defined
- Escalation paths documented
- Change management capability assessed
- Training requirements identified

**Risk Indicators:** - Reliance on tribal knowledge. No internal documentation

## 7. Modernization Strategy Alignment

**Objective:** Ensure technology decisions support long-term goals.

- Desired future-state architecture defined
- Timeline realism validated
- Budget alignment confirmed
- Risk tolerance agreed upon by leadership

**Risk Indicators:** - Binary "stay or rip-and-replace" thinking, no phased transition plan

## 8. Security, Compliance & Risk Governance

**Objective:** Ensure communications infrastructure aligns with organizational security and compliance requirements

- Voice and UC infrastructure included in cybersecurity risk assessments
- Applicable regulatory obligations identified (e.g., healthcare, education, public sector)
- Logging, monitoring, and incident response responsibilities defined
- Third-party and administrative access reviewed and documented

**Risk Indicators:** - Voice systems excluded from security reviews - Undefined incident response ownership

## 9. Business Impact Assessment

**Objective:** Translate technical risk into business impact.

- Operational impact of a voice outage understood
- Teams, services, or customers affected by disruption identified
- Acceptable downtime thresholds defined
- Financial, safety, or reputational risk assessed

**Risk Indicators:** No quantified impact of downtime. Misalignment between IT and business leadership expectations

## 10. Ownership & Accountability

**Objective:** Establish clear responsibility for communications outcomes.

Platform owner (role): \_\_\_\_\_

Partner or vendor escalation path defined:  Yes  No

Change approval authority defined:  Yes  No

**Risk Indicators:** - Diffuse or informal ownership. Reliance on tribal knowledge

## Executive Summary (To Be Completed After Review)

Overall Readiness:  High  Moderate  Needs Attention

Primary Risks Identified:

Recommended Next Actions:

*This assessment is intended to support defensible decision-making. Whether the outcome is to maintain, modernize, integrate, or migrate, the goal is to ensure decisions are based on operational reality rather than urgency or assumption.*

---

*This document reflects how experienced communications operators evaluate Mitel environments in 2026 – focusing on continuity, risk, and business alignment rather than platform marketing.*