



Mountain Line 5-Year Strategic Technology Plan (Fiscal Years 2027-2032)

Table of Contents

Executive Summary	6
Strategic Investment Framework	7
Mission Alignment	7
Critical Success Factors	7
Strategic Context	7
Organizational Overview	7
Current Operating Environment	7
Technology Maturity Assessment	8
Technology Environment Assessment	8
Strategic Alignment	9
Federal Transit Administration (FTA) Alignment	9
FTA Grant Eligibility and Compliance	9
Transit Asset Management (TAM) Integration	9
Public Transportation Agency Safety Plan (PTASP) Support	9
Civil Rights and Equity Compliance	9
State and Regional Alignment	10
Arizona Department of Transportation (ADOT) Coordination	10
MetroPlan Integration	10
Industry Best Practices and Standards Alignment	10
American Public Transportation Association (APTA) Standards	10
NIST Cybersecurity Framework	10
Transportation Security Administration (TSA) Requirements	10
Cloud Security and Data Protection	11
Strategic Goals and Objectives	11
Goal 1: Data Integration & Business Intelligence	11
Current State Challenges:	11
Objective 1.1: Implement Enterprise Data Warehouse	11

Technical Architecture Components:.....	11
Data Warehouse Architecture Layers:	11
Implementation Approach:	12
Data Governance Framework:	13
Success Metrics:	14
Budget Estimate:	14
Objective 1.2: Real-Time Operational Dashboards	14
Dashboard Portfolio (with example data points):.....	14
Dashboard Design Principles:.....	16
Implementation Timeline:.....	16
Budget Estimate:	16
Goal 2: System Modernization & Integration	17
Objective 2.1: Replace Fare Collection System	17
Risk Mitigation:.....	17
Success Metrics:	17
Goal 3: Governance & Policy Framework	17
Objective 3.1: Establish Technology Steering Committee	17
Committee Structure:	18
Meeting Cadence and Agenda:	18
Decision-Making Authority:	18
Documentation and Transparency:.....	18
Objective 3.2: Develop Comprehensive Technology Policies	19
Policy Portfolio:	19
1. Acceptable Use Policy (AUP)	19
2. Data Governance and Privacy Policy	19
3. Cybersecurity Policy	20
4. System Backup and Disaster Recovery Policy	20
6. Change Management Policy and Procedure	20
Policy Development and Approval Process:.....	21
Policy Review and Updates:	21
Success Metrics:	22
Objective 3.3: Implement Change Management Framework.....	22
ADKAR Elements Applied to Mountain Line:	22
Change Management Process for Major Technology Projects:	23
Change Management Roles:	24
Success Metrics:	25

Budget Estimate: 25

Objective 3.4: Develop Business Continuity and Disaster Recovery Plan 25

 Business Continuity Plan (BCP) vs. Disaster Recovery Plan (DRP):..... 25

 Critical Business Functions (Mountain Line): 26

 IT Systems Recovery Priorities: 26

 Disaster Scenarios and Response:..... 27

 Plan Development and Maintenance:..... 29

 Alignment with Regional Plans:..... 29

 Success Metrics: 30

 Budget Estimate: 30

Goal 4: Infrastructure & Operations Excellence..... 30

 Objective 4.1: Modernize Network and Infrastructure..... 30

 Current State Assessment: 30

 Infrastructure Modernization Components:..... 30

 1. Inter-Facility Connectivity 30

 2. Network Equipment Refresh 31

 3. Cloud Migration Strategy 31

 4. Server and Storage Infrastructure..... 32

 Objective 4.2: Strengthen Cybersecurity Posture 33

 Cybersecurity Improvement Roadmap: 33

 Objective 4.3: Establish Sustainable IT Support Model 37

 Current State Challenges:..... 38

 Target State: 38

 Staffing Strategy:..... 38

 Hiring Timeline: 39

 Recruiting Strategy:..... 39

 Retention Strategy: 39

 IT Service Management (ITSM) Implementation: 39

 Service Desk Processes:..... 40

 Priority Levels and SLAs: (Note: Response and Resolution Times are business hours/days.) 40

 Knowledge Base: 40

 User Communication:..... 41

 Success Metrics: 41

 Budget Estimate: 41

Goal 5: Security, Compliance & Risk Management..... 41

 Objective 5.1: Data-Driven Service Planning and Performance Measurement..... 41

Service Planning Applications: 41

Objective 5.2: Accessibility and Equity in Technology 44

 Accessibility Standards and Compliance: 44

Technology Risk Assessment and Mitigation 46

 Risk 1: Cybersecurity Incident (Ransomware, Data Breach, OT Attack) 46

 Impact: 46

 Mitigation Strategies: 48

 Risk 2: IT Staffing Gaps and Turnover 49

 Impact: 49

 Mitigation Strategies: 50

 Success Criteria: 50

 Risk 3: Budget Funding Gaps and Grant Delays 51

 Impact: 51

 Mitigation Strategies: 51

 Success Criteria: 51

Emerging Risks (Lower probability, but significant impact if occur) 52

 Risk 4: Vendor Business Failure or Abandonment (Probability: 5%) 52

 Risk 5: Technology Obsolescence (Probability: 20%) 52

Continuous Improvement Process 53

 Annual Strategic Review: 53

 Post-Implementation Reviews: 53

Conclusion 54

Appendix A: Implementation Roadmap & Phasing..... 55

 Multi-Year Implementation Phasing and Dependencies 55

 Phase 1: Foundation & Quick Wins (Year 1)..... 55

 Phase 2: System Modernization & Integration (Year 2)..... 55

 Phase 3: Advanced Analytics & Operational Technology Security (Year 3) 56

 Phase 4: Optimization & Continuous Improvement (Years 4-5) 56

Appendix B: Key Budget Drivers by Category 58

 Personnel (largest recurring cost):..... 58

 Major System Implementations (one-time capital): 58

 Ongoing Operating Costs (annual subscriptions/support):..... 58

Appendix C: Funding Strategies 59

 Primary Funding Sources:..... 59

 Potential Grant Application Strategies..... 61

 Budget Management and Tracking 61

Executive Summary

This 5-Year Technology Strategic Plan establishes a practical roadmap for modernizing Mountain Line’s technology environment from FY 2027 through FY 2031. It responds to the agency’s current operating reality: growing service expectations, two-facility operations, zero-emission fleet transition, increasing cybersecurity risk, and a fragmented application landscape with more than 30 systems that are not consistently integrated. The plan is designed to move Mountain Line from reactive, system-by-system technology management toward a coordinated enterprise model in which data, applications, infrastructure, cybersecurity, and governance are treated as strategic assets that directly support safe, reliable, accessible, and sustainable public transportation.

The plan’s highest priorities are data integration, system modernization, operational resilience, and cybersecurity maturity. A central recommendation is the creation of an enterprise data warehouse and business intelligence environment that can integrate operations, maintenance, finance, safety, fare collection, paratransit, planning, and energy data into a reliable source of truth for reporting and decision-making. This foundation will reduce manual reporting, support FTA and Board reporting, and enable real-time dashboards for executives, managers, dispatchers, maintenance leaders, finance staff, safety teams, and customer experience functions. Parallel modernization efforts include replacing or improving key systems such as fare collection, fleet management, HR-related workflows, camera/video systems, and cloud-based infrastructure so that Mountain Line can improve reliability, reduce duplicate work, and better connect technology investments to operational outcomes.

Successful execution will require disciplined oversight, adequate staffing, and phased investment. The plan recommends a Technology Steering Committee, formal data governance, comprehensive technology policies, change management practices, and a business continuity/disaster recovery framework to ensure that projects are prioritized, funded, implemented, and sustained consistently. It also identifies IT bench strength as a critical risk and calls for the addition of data analytics and support capacity to relieve unsustainable workloads, improve service desk performance, and support major initiatives. Across the five-year period, the plan anticipates a strategic technology investment of approximately \$3-\$3.5 million, aligned where possible with FTA formula and discretionary grant opportunities, state and regional partnerships, and local match planning.

By Year 5 of this plan, Mountain Line will have a more integrated, secure, data-driven, and resilient technology environment that improves both internal operations and rider experience. Expected outcomes include stronger cybersecurity alignment with TSA directives and NIST frameworks, improved network and cloud reliability across the Kaspar and the Downtown Connection Center locations, more accessible and equitable rider-facing technologies, better support for zero-emission fleet operations, faster and more accurate reporting, and more consistent technology decision-making. Most importantly, the plan positions technology as an agency-wide enabler of service excellence, employee investment, financial stability, and community value—helping Mountain Line deliver better mobility for Flagstaff while responsibly stewarding public resources and preparing for future growth.

Strategic Investment Framework

This plan is strategically aligned with Federal Transit Administration (FTA) grant opportunities, particularly Section 5307 (Urbanized Area Formula Grants), Section 5339 (Bus and Bus Facilities Program), and emerging Bipartisan Infrastructure Law (BIL) technology funding. The phased implementation approach ensures alignment with Mountain Line's operational priorities, funding cycles, and organizational capacity.

Mission Alignment

Technology investments detailed in this plan directly support Mountain Line's core mission to provide safe, reliable, accessible, and sustainable public transportation services to the Flagstaff community. Each initiative maps to one or more of the following success outcomes:

- Service Excellence
- Employee Investment
- Financial Stability
- Community Value

Critical Success Factors

Achievement of this plan's objectives depends on:

1. **Executive Leadership Commitment:** Sustained CEO and Board support for multi-year technology transformation
2. **Adequate Staffing:** Filling critical positions (IT Technician, Data Analyst,) and maintaining appropriate vendor partnerships
3. **Grant Funding Success:** Securing federal and state technology grants aligned with project timelines
4. **Governance Framework:** Establishing technology steering committee and decision-making structures
5. **Change Management:** Effective communication, training, and stakeholder engagement throughout implementations
6. **Vendor Partnerships:** Strategic selection of technology partners with transit industry expertise and long-term viability

Strategic Context

Organizational Overview

Mountain Line is a public transit agency serving Flagstaff, Arizona, and surrounding areas. Its operations span fixed-route, paratransit, microtransit, and regional mobility services. Technology investments are managed collaboratively with input from cross-functional business stakeholders.

Current Operating Environment

Mountain Line operates in a dynamic environment characterized by:

Service Growth Demands: Following voter approval of increased transit funding, Mountain Line faces expectations to expand service coverage and frequency while maintaining financial sustainability. Technology must enable the agency to "do more with less" through operational efficiency gains.

Two-Facility Operations: The June 2025 opening of the Downtown Connection Center (DCC) alongside the existing Kaspar Drive facility creates dual-site operational complexity requiring robust network connectivity, distributed IT support, and unified system access across locations.

Fleet Modernization: Transition to zero-emission buses (current: 1 Gillig EV and 1 New Flyer EV, with expansion planned) requires integrated charging infrastructure management, specialized maintenance diagnostics, and energy optimization systems.

Workforce Challenges: Like transit agencies nationwide, Mountain Line faces operator recruitment and retention challenges requiring modern HR systems, improved training tools (bus simulator implemented September 2025), and competitive technology-enabled work environment.

Cybersecurity Threats: Transit agencies face increasing cyber risks from nation-state actors, ransomware gangs, and hackers targeting both information technology (IT) and operational technology (OT) systems. Mountain Line must mature from reactive to proactive security posture.

Technology Maturity Assessment

Current State Maturity Scoring (1-5 scale, 5=optimized)

Domain	Current Maturity	Target (Year 5)	Priority
System Integration	2 - Initial	4 - Managed	Critical
Data & Analytics	2 - Initial	4 - Managed	Critical
IT Governance	1 - Ad-hoc	4 - Managed	Critical
Cybersecurity	2 - Initial	4 - Managed	High
Cloud Infrastructure	2 - Initial	4 - Managed	High
Application Portfolio	3 - Defined	4 - Managed	Medium
IT Service Management	3 - Defined	4 - Managed	Medium
Disaster Recovery	2 - Initial	4 - Managed	High

Assessment Basis: Maturity scoring based on CMMI (Capability Maturity Model Integration) framework adapted for transit technology environments, informed by October 2025 stakeholder assessments and system inventory analysis.

Technology Environment Assessment

A technical assessment highlighted a highly fragmented system landscape, weak system integrations, critical legacy data persistence needs, and absence of coordinated business intelligence, project management, and IT policy/guidance

mechanisms. Cybersecurity maturity remains emergent, and staff training for new systems is critical. Several prioritized capital projects, such as transitioning to zero-emission vehicles, require robust technology support and integration.

Strategic Alignment

Plan objectives directly align with Board and executive priorities, the agency's sustainability directives, as well as FTA and regional public sector best practices. The strategy accounts for ongoing regulatory compliance, funding requirements, and evolving community needs.

Federal Transit Administration (FTA) Alignment

FTA Grant Eligibility and Compliance

All technology initiatives in this plan align with FTA capital and operating grant eligibility requirements under:

- **49 U.S.C. § 5307** - Urbanized Area Formula Grants (primary Mountain Line funding source)
- **49 U.S.C. § 5339** - Bus and Bus Facilities Program (capital equipment including technology infrastructure)
- **49 U.S.C. § 5310** - Enhanced Mobility of Seniors and Individuals with Disabilities (paratransit technology integration)
- 5305e - Planning

Transit Asset Management (TAM) Integration

Per FTA regulations (49 CFR Part 625), Mountain Line must maintain a Transit Asset Management Plan. Technology investments support TAM objectives through:

- Enhanced asset tracking and condition monitoring (ThingTech, fleet management systems)
- Data-driven capital planning and replacement scheduling
- Performance measurement aligned with State of Good Repair (SGR) metrics
- Integration between asset management and financial systems for lifecycle cost analysis

Public Transportation Agency Safety Plan (PTASP) Support

Technology initiatives support Mountain Line's Safety Management System (SMS) required under 49 CFR Part 673:

- Incident reporting and management integration (Elerts/See Say, camera systems, HR tracking)
- Safety performance monitoring and trending
- Operator training tracking and certification management
- Hazard identification through data analytics

Civil Rights and Equity Compliance

Technology procurements and implementations comply with:

- **Title VI of the Civil Rights Act** - ensuring technology benefits are equitably distributed across service areas and demographic groups
- **ADA (Americans with Disabilities Act)** - ensuring accessible technology interfaces, announcements, and rider information

- **DBE (Disadvantaged Business Enterprise)** - technology procurements include DBE participation goals per Mountain Line's FTA-approved DBE program
- **Limited English Proficiency (LEP)** - multilingual support in customer-facing technologies

State and Regional Alignment

Arizona Department of Transportation (ADOT) Coordination

- Leveraging ADOT/DHS-provided cybersecurity tools (CrowdStrike, Tanium)
- Alignment with statewide transit technology standards where applicable
- Coordination on regional mobility and data sharing initiatives

MetroPlan Integration

As the Flagstaff Metropolitan Planning Organization (MPO), MetroPlan partnerships include:

- Regional transportation data sharing for planning analyses
- Coordinated transit-human services transportation planning
- Technology supporting Coordinated Plan objectives (connectivity, efficiency, information access)

Industry Best Practices and Standards Alignment

American Public Transportation Association (APTA) Standards

Technology planning incorporates relevant APTA standards:

- **APTA SS-ECS-RP-001-14** - Cybersecurity Considerations for Public Transit
- **APTA SS-CCS-RP-006-23** - Operational Technology Cybersecurity Maturity Framework (OT-CMF)
- **APTA IT-RRTS-RP-003-08** - Business Continuity and Disaster Recovery Planning
- **APTA CC-GDSTM-RP-001-12** - General Transit Feed Specification (GTFS) and Real-Time Information Standards

NIST Cybersecurity Framework

Cybersecurity initiatives align with:

- **NIST Cybersecurity Framework 2.0** core functions (Govern, Identify, Protect, Detect, Respond, Recover)
- **NIST CSWP 51** - Transit Cybersecurity Framework Community Profile (in development)
- **NIST SP 800-171** - Protecting Controlled Unclassified Information in nonfederal systems

Transportation Security Administration (TSA) Requirements

Compliance with **TSA Security Directive 1580-21-01** (December 2021) requiring:

- Designated Cybersecurity Coordinator
- Cyber incident reporting to CISA within 24 hours
- Cybersecurity Incident Response Plan
- Cybersecurity Vulnerability Assessment

Cloud Security and Data Protection

- **FedRAMP** (Federal Risk and Authorization Management Program) compliance for cloud services handling FTA data
- **NIST SP 800-53** security controls for information systems
- **PCI-DSS** (Payment Card Industry Data Security Standard) for systems handling credit card data

Strategic Goals and Objectives

Goal 1: Data Integration & Business Intelligence

Strategic Objective: Establish a unified data platform that integrates disparate operational, maintenance, financial, and customer service systems to enable data-driven decision-making, eliminate manual reporting workarounds, and preserve institutional knowledge.

Current State Challenges:

- Lack of true data management platform creates a critical business intelligence gap
- Lack of understanding and utilization of full capabilities of currently used platforms
- 30+ disconnected systems with minimal integration
- Manual report generation consuming significant staff time
- Inability to correlate cross-functional data (maintenance impacts on service reliability, charging efficiency on fleet availability)
- Limited visibility into performance metrics for grant reporting and board communication

Objective 1.1: Implement Enterprise Data Warehouse

Description: Deploy modern data warehouse infrastructure or a business analytics platform to serve as single source of truth for analytical reporting, performance management, and business intelligence.

Technical Architecture Components:

Data Warehouse Platform Selection Criteria:

- **Cloud-based**
- **Scalability** to handle growing data volumes from EVs, sensors, and expanded operations
- **Transit-specific** dimensional models (route-day-vehicle hierarchies)
- **Real-time and batch** data ingestion capabilities
- **FTA reporting alignment** (NTD, DBE, TAM, PTASP metrics)
- **Open architecture** supporting multiple BI tools and APIs

Data Warehouse Architecture Layers:

Layer 1 - Data Sources (Extraction):

- **Operations:** GMV CAD/AVL, Optibus, Transit app, CradlePoint, Spare Labs
- **Maintenance:** RTA Fleet, ThingTech, Ford IDS, Allison, ABB, ChargePoint

- **Safety:** REI, Elerts, security camera systems
- **Finance:** Fare collection system, Sage/RAMP, Square
- **Customer Service:** Complaints/Compliments database, Elerts
- **HR:** Inflection
- **Planning:** Remix, Optibus

Layer 2 - Staging & ETL (Extract, Transform, Load) and ELT (Extract, Load, Transform):

- **Landing zone** for raw data ingestion (preserve source data integrity)
- **Data quality validation** (completeness, accuracy, timeliness checks)
- **ETL processing** using Azure Data Factory, Informatica, Talend, or similar
- **Error handling and logging** for failed integration jobs
- **Incremental load processing** to minimize performance impact on operational systems

Layer 3 - Core Data Warehouse (Dimensional Model):

- **Fact tables:** Vehicle trips, maintenance work orders, fare transactions, incidents, energy consumption
- **Dimension tables:** Routes, vehicles, operators, locations, time/date, fare products, equipment
- **Slowly changing dimensions (SCD)** to track historical changes (route modifications, vehicle reassignments)
- **Conformed dimensions** enabling cross-functional analysis

Layer 4 - Data Marts (Subject Areas):

- **Operations data mart:** On-time performance, service delivery, ridership
- **Maintenance data mart:** Work orders, parts inventory, vehicle reliability, lifecycle costs
- **Financial data mart:** Revenue, expenses, cost allocation, grant tracking
- **Safety data mart:** Incidents, training, certifications, compliance
- **Energy data mart:** EV charging, fuel consumption, efficiency metrics

Layer 5 - Analytics & Presentation:

- **Self-service BI tools:** Power BI, Tableau, or similar
- **Dashboards** for executives, managers, and analysts
- **Standard reports** (FTA NTD, board reports, grant reports)
- **Ad-hoc query** capabilities for power users
- **Mobile access** for field staff and executives

Implementation Approach:

Phase 1: Foundation

- Platform selection and procurement

- Architecture design and documentation
- Cloud infrastructure setup (Azure resource groups, networking, security)
- Establish data governance committee
- Define data dictionary and business glossary

Phase 2: Priority Integrations

- Integrate GMV CAD/AVL operational data (highest volume, most stakeholder demand)
- Integrate Sage/RAMP financial data (critical for budget and grant reporting)
- Develop initial Operations Dashboard (OTP, ridership, service hours)
- Develop initial Financial Dashboard (revenue, expenses, cost per hour)

Phase 3: Fleet and Maintenance

- Integrate RTA fleet management system
- Integrate ThingTech asset management data
- Develop Maintenance Dashboard (work orders, vehicle availability, lifecycle costs)

Phase 4: Additional Systems

- Integrate fare collection system data
- Integrate safety and security system data (cameras, incidents, training)
- Integrate EV charging data for energy optimization
- Develop Safety Dashboard and Energy Management Dashboard

Data Governance Framework:

Establish formal data governance to ensure data quality, security, and appropriate use:

Data Governance Committee:

- **Executive Sponsor:** CEO/GM
- **Data Steward (Chair):** IT Manager
- **Business Data Owners:** Department heads for Operations, Maintenance, Finance, HR, Planning, Administration
- **Technical Data Custodian:** Data Analyst (to be hired; handled by Strategic Performance Planner short-term)
- **Quarterly meetings** to review data quality, resolve issues, approve new integrations
- **Note:** initially Data Governance Committee duties can be taken on by the Technology Steering Committee, until such time as separate committees are required.

Data Governance Policies:

- **Data ownership** - defining which department owns each data domain
- **Data quality standards** - acceptable completeness, accuracy, timeliness thresholds
- **Data access controls** - role-based access to sensitive data (HR, financial, security)

- **Data retention** - how long data is kept in active warehouse vs. archived
- **Data privacy** - protecting rider PII, employee information per GDPR-like principles
- **Data classification** - public, internal, confidential, restricted tiers

Success Metrics:

- **Reduce manual reporting time** by 60% (baseline: staff time surveys)
- **Increase data accessibility** - 90% of standard reports available via self-service dashboards within 18 months
- **Improve decision cycle time** - reduce time from question to insight from days/weeks to hours/same-day
- **FTA NTD reporting accuracy** - zero major findings or data revisions in FTA audits
- **User adoption** - 80% of managers and analysts actively using BI tools within 24 months
- **Data quality** - achieve 95%+ completeness and accuracy scores for critical data elements

Budget Estimate:

- **Platform licensing:** \$40-80K annually (depending on data volume and user count)
- **Integration tools/ETL:** \$30-50K annually
- **BI tool licensing:** \$20-40K annually
- **Implementation services:** \$200-350K (consultant support for design and initial integrations)
- **Ongoing maintenance:** \$100-121K annually (data analyst salary, tool maintenance)
- **Total 5-year investment:** \$650K - \$1.1M

Objective 1.2: Real-Time Operational Dashboards

Description: Develop or procure executive, operational, and departmental dashboards providing real-time visibility into key performance indicators.

Dashboard Portfolio (with example data points):

Executive Dashboard (CEO, Deputy GM, Board):

- **Daily service delivery:** Total revenue hours, revenue miles, OTP (early vs. Late), major delays/detours, missed trips
- **Ridership trends:** Daily/weekly/monthly ridership vs. plan, year-over-year comparison
- **Financial snapshot:** Farebox recovery, revenue vs. budget, key expense categories
- **Fleet availability:** Vehicles in service, out for maintenance, EV charging status, PM compliance
- **Safety summary:** Incidents (by type), days since last preventable accident, training compliance, pre-trip inspection compliance
- **Key projects status:** Technology plan milestones, capital projects, procurement timelines
- **Alerts:** Critical issues requiring executive attention (system outages, major incidents, compliance risks)
- **Headcount:** by department (budget vs. Actual vs pipeline)

- **Customer Complaints:** complaints per 10,000 riders

Operations Dashboard (Deputy GM of Operations, Dispatchers, Planners):

- **Real-time service monitoring:** Vehicle locations, current OTP by route, active delays
- **Operator status:** Clock-ins, assignments, break compliance, run-board adjustments. Attendance stats to include tot
- **Service alerts:** Detours, disruptions, weather impacts, special events
- **Ridership demand:** Current passenger loads (APC data), hot spots, capacity utilization
- **Tomorrow's service:** Scheduled blocks, operator assignments, vehicle assignments
- **Historical performance:** Route-level OTP trends, reliability metrics, schedule adherence
- **Accessibility metrics:** ADA paratransit performance, lift/ramp availability

Maintenance Dashboard (Maintenance Superintendent, Technicians):

- **Fleet status:** Vehicles available, in maintenance, out of service, EV charging. List vehicles available by type (60', 40', BEB). PM's for the day. Need a comprehensive down bus list which needs to be updated in real-time that looks at PM, long term OOS and any bus off property with vendors.
- **Work orders:** Open/pending/completed, overdue PMs, priority repairs
- **Parts inventory:** Stock levels and total price of inventory. Reorder points, backorders, high-usage parts, inventory value vs. expectation.
- **Vehicle health:** Fault codes, diagnostic alerts, upcoming PM schedules, MTBF (Mean Time Between Failure) or miles between road calls is a better standard. prediction
- **Labor utilization:** Technician assignments, work order cycle time, productivity metrics.
- **Lifecycle management:** Vehicle age, mileage, replacement planning, warranty expirations and management
- **EV-specific metrics:** Battery health, charging cycles, range degradation, energy efficiency
- **Deferred maintenance** – PM identified defects vs. Actual defects completed (what is left over is deferred and needs to be track
- **Repeaters** – bus breaks vs the reason why it occurred. If you have a bus breakdown for the same or similar issue within 30 days you have a repeat failure which shows a lack of diagnostic capacity, training issue

Finance Dashboard (Finance Manager, Budget Analysts):

- **Revenue tracking:** Farebox, pass sales, grants drawn, miscellaneous revenue vs. budget
- **Expense monitoring:** Payroll, fuel, parts, insurance, utilities vs. budget by cost center
- **Grant management:** Available balances, expenditure rates, close-out deadlines, matching requirements
- **Cost allocation:** Cost per revenue hour, cost per passenger, cost per mile by service type
- **Accounts payable/receivable:** Aging, cash flow projections
- **Budget variance:** Monthly and YTD variance analysis with drill-down capabilities

Safety & Training Dashboard (Safety and Training Director, Safety Committee):

- **Incident tracking:** By type (preventable accidents, customer incidents, employee injuries), trends, severity need the following metrics Preventable Accident Frequency Ration (PAFR). Accident Frequency Ration AFR, Preventable injury ration (PIFR) and injury ration frequency (IFR)
- **Training compliance:** Certifications current/expiring, refresher training due, simulator utilization. Headcount in training and their status. Need a metric to track how long new employees are in training vs. expectation. Looking to see how safe and quick we are turning the pipeline
- **Operator performance:** Safe driving scores, incident history, commendations (OTP by OP, Accidents, Attendance
- **Vehicle inspections:** Pre-trip compliance, defect identification and resolution (we need to ensure the quality of the pre-trip. Not sure if we have the tools/resources to do so
- **Worker compensation:** Open claims, costs, return-to-work status
- **Regulatory compliance:** FTA Safety Plan metrics, OSHA recordables, drug/alcohol testing compliance

Customer Experience Dashboard (Deputy GM, Marketing, Customer Service):

- **Ridership patterns:** By route, time of day, day of week, demographic segments
- **Fare media usage:** Mobile app transactions, cash fares, pass types, fare capping
- **Customer feedback:** Compliments, complaints, suggestions by category and trend
- **Real-time information accuracy:** Transit App data quality, sign/announcements functioning
- **Accessibility metrics:** accessibility complaints
- **Marketing campaign effectiveness:** Ridership response to promotions, outreach ROI

Dashboard Design Principles:

- **Mobile-responsive:** Accessible on tablets and smartphones for field staff
- **Role-based access:** Show relevant KPIs and data for each user's responsibilities
- **Drill-down capabilities:** Click through from summary to detail for investigation
- **Actionable alerts:** Highlight exceptions requiring attention, not just data displays
- **Refresh frequency:** Real-time for operational data, daily/weekly for financial and safety data
- **Export capabilities:** Download to Excel/PDF for sharing and offline analysis

Implementation Timeline:

- **Phase 1:** Finance and Operations dashboards (highest demand)
- **Phase 2:** Maintenance and Executive dashboards
- **Phase 3:** Safety and Customer Experience dashboards
- **Ongoing:** Continuous refinement based on user feedback

Budget Estimate: Included in data warehouse implementation budget (BI tool licensing covers dashboard development)

Goal 2: System Modernization & Integration

Strategic Objective: Replace aging legacy systems with modern, cloud-based, integrated technologies that improve operational efficiency, enhance data quality, support zero-emission vehicle transition, and reduce total cost of ownership.

Objective 2.1: Replace Fare Collection System

Priority: CRITICAL - URGENT (Target: Summer 2027 implementation)

Current State: The current electronic fare collection system is 12 years old and has been outgrown. There is poor integration between existing electronic and mobile fare collection systems, and limited functionality for modern fare strategies with limited vendor support. RFP was conducted in spring of 2026, and Masabi was identified as the best solution for Mountain Line’s needs. What follows are considerations Mountain Line will want to keep in mind moving into the planning and implementation phases.

Risk Mitigation:

- **Revenue protection:** Immediate cutover with contingency plans. Also relies on the four items below.
- **Operator training:** Comprehensive training before rollout to avoid passenger confusion and delays
- **Public communication:** 90-day advance notice to riders, multilingual materials, onboard announcements
- **Vendor accountability:** Performance guarantees, liquidated damages for late delivery or system failures
- **Grant compliance:** Ensure all procurement steps meet FTA requirements to protect federal funding

Success Metrics:

- **Boarding time reduction:** 10% faster average boarding time improving schedule adherence
- **Fare evasion reduction:** Improved fare compliance through easier payment and enforcement
- **Mobile adoption:** 45% of transactions via mobile/contactless within 12 months of launch (assuming paper day passes are no longer sold on board)
- **Rider satisfaction:** 85%+ satisfaction with ease of payment in post-implementation survey
- **Revenue reconciliation:** 100% automated daily reconciliation eliminating manual spreadsheets
- **System uptime:** 99.5%+ availability, <2 hours downtime per year

Goal 3: Governance & Policy Framework

Strategic Objective: Establish formal technology governance structures, policies, and procedures to guide investment decisions, manage change effectively, ensure cybersecurity, and align technology initiatives with organizational priorities and federal compliance requirements.

Objective 3.1: Establish Technology Steering Committee

Description: Create formal governance body with executive leadership, department heads, and technical staff to oversee technology strategy, prioritize investments, and resolve cross-functional technology decisions.

Committee Structure:

Technology Steering Committee Composition:

- **Executive Sponsor:** CEO/GM provides leadership authority, budget approval, strategic alignment
- **Chair:** IT Manager - technical feasibility, resource requirements, vendor management-
- **Permanent Members:**
 - Deputy General Manager of Administration - service delivery impacts, change management leadership
 - Deputy General Manager of Operations- operational priorities, dispatcher/operator needs
 - Facilities & Maintenance Manager - fleet and facilities systems requirements, technician workflows
 - Finance Director - budget implications, grant funding, ROI analysis
 - Planning Director - data analytics needs, performance measurement, strategic planning alignment
 - HR Manager - HR system requirements
 - Safety and Training Director - training needs, safety compliance
 - Purchasing/Contracts Officer - procurement processes, vendor contracting
- **Ad-Hoc Members** (invited based on agenda topics):
 - Marketing/Communications staff - customer-facing technology, public information systems
 - Planning staff – service planning needs
 - Systems Administrator – integration and compatibility questions
 - Transit Safety Specialist - safety system integration, incident management technology
 - External consultants - specialized expertise, independent assessment

Meeting Cadence and Agenda:

- **Quarterly meetings** (minimum)
- **Special meetings** as needed for urgent decisions (major system failures, urgent procurements, grant deadlines)

Decision-Making Authority:

Committee Authority:

- **Prioritize competing technology requests** when budget/staff capacity is constrained
- **Establish technology policies and standards** (acceptable use, data governance, security)
- **Resolve cross-departmental conflicts** related to technology requirements or resources

Documentation and Transparency:

- **Meeting minutes** distributed to all members within 5 business days
- **Action item tracking** with assigned owners and due dates

- **Decision log** maintained by IT Manager documenting key technology decisions, rationale, outcomes

Objective 3.2: Develop Comprehensive Technology Policies

Description: Document formal policies governing technology use, data management, cybersecurity, and procurement to ensure consistency, compliance, and accountability.

Policy Portfolio:

1. Acceptable Use Policy (AUP)

Purpose: Define appropriate use of Mountain Line technology resources (computers, mobile devices, email, internet access, network) by employees, contractors, and authorized users.

Operational Policy: handled as part of Personnel Policy Manual.

Key Policy Elements:

- **Authorized use:** Business purposes, incidental personal use guidelines
- **Prohibited activities:** Illegal activity, harassment, personal business ventures, excessive personal use, gambling, pornography
- **Email and communications:** Professional standards, public records retention, no expectation of privacy
- **Internet access:** Allowed sites, blocked categories, monitoring disclosure
- **Mobile device use:** Personal vs. agency-owned devices, Bring Your Own Device (BYOD) standards
- **Social media:** Official vs. personal accounts, Mountain Line branding, crisis communication protocols
- **Enforcement:** Progressive discipline for violations (verbal warning, written warning, suspension of access, termination)

2. Data Governance and Privacy Policy

Purpose: Establish rules for collecting, storing, using, and protecting data, balancing operational needs with privacy rights and compliance obligations.

Key Policy Elements:

- **Data classification:** Public, internal, confidential, restricted (PII, financial, HR, security)
- **Data ownership:** Assign data stewardship to department heads for their functional areas
- **Data quality standards:** Completeness, accuracy, timeliness, consistency requirements
- **Data retention:** How long different data types are kept, aligned with FTA requirements (minimum 3 years for grant documentation, 7 years for property records) and Arizona public records laws
- **Data access controls:** Role-based access, least privilege principle, segregation of duties
- **Privacy protections:** Rider PII (names, addresses, payment card data), employee records, video footage with faces
- **Data breach response:** Notification procedures, containment actions, investigation, remediation
- **Third-party data sharing:** Vendor contracts must include data protection clauses, limited use restrictions, breach notification requirements

3. Cybersecurity Policy

Purpose: Protect Mountain Line's information technology systems and operational technology from cyber threats, aligned with TSA Security Directive 1580-21-01 and NIST Cybersecurity Framework.

Key Policy Elements:

- **Cybersecurity Coordinator:** IT Manager designated as responsible official, reports cyber incidents to CEO and CISA within 24 hours per TSA requirements
- **Access controls:** Strong password requirements (align with current NIST recommendations), multi-factor authentication (MFA) for remote access and privileged accounts
- **Endpoint protection:** Antivirus/anti-malware (CrowdStrike provided by AZDoHS), automatic updates, device encryption
- **Network security:** Firewall rules, network segmentation (separate guest Wi-Fi from operations), intrusion detection/prevention
- **Vulnerability management:** Regular patching (critical patches within 15 days, high-risk within 30 days), ongoing vulnerability scans
- **Security awareness training:** Mandatory training for all new staff, monthly phishing simulation exercises, bi-monthly refresher training
- **Incident response plan:** Detection, containment, eradication, recovery, lessons learned
- **Physical security:** Server room access controls, visitor logs, camera coverage, equipment disposal (data wiping/destruction)

4. System Backup and Disaster Recovery Policy

Purpose: Ensure critical data and systems can be recovered following hardware failure, natural disaster, cyberattack, or other disruption.

Key Policy Elements:

- **Backup scope:** All critical systems and data (financial, HR, operations, maintenance, email, file shares)
- **Backup frequency:** Daily incremental backups, weekly full backups, monthly full backups
- **Backup retention:** Incremental backup retained for 1 week, weekly full backup retained for 1 month, monthly full backup retained for 12 months
- **Backup testing:** Weekly restoration tests to verify backups are viable
- **Recovery Time Objective (RTO):** Target time to restore service (varies by system criticality - see Objective 3.4)
- **Recovery Point Objective (RPO):** Maximum tolerable data loss (varies by system – ex: financial systems 1 day, email 1 day, operations data 1 hour)
- **Offsite storage:** Cloud backup with geographic redundancy, encrypted in transit and at rest, with immutable options

6. Change Management Policy and Procedure

Purpose: Minimize disruption and risk when implementing technology changes (system upgrades, configuration changes, new deployments).

Key Policy Elements:

- **Change categories:**
 - **Standard changes:** Pre-approved, low-risk, routine (password resets, equipment swaps) - IT Manager approval
 - **Normal changes:** Moderate risk, require testing and approval - Technology Steering Committee or CEO/IT Manager approval
 - **Emergency changes:** Urgent fixes to restore service or address security threats - CEO/IT Manager approval with post-implementation review
- **Change request process:** Documented business justification, technical design, risk assessment, rollback plan, testing results
- **Change windows:** Scheduled maintenance windows (ex: Saturday nights 10pm-6am) for planned changes to minimize operational impact
- **Communication:** Advance notice to affected users, status updates during implementation, post-implementation confirmation
- **Documentation:** Change logs maintained in IT ticketing system, configuration management database (CMDB) updated

Policy Development and Approval Process:

Phase 1: Drafting (Months 1-3)

- IT Manager leads policy development with input from department heads and legal review
- Benchmark policies from comparable transit agencies (peer best practices)
- Align with FTA, TSA, NIST, and APTA standards where applicable

Phase 2: Review and Revision (Months 4-5)

- Technology Steering Committee reviews draft policies
- Legal counsel review for compliance with Arizona law, federal regulations, labor agreements
- Staff feedback sessions to ensure policies are practical and understandable

Phase 3: Approval and Implementation (Months 6-12)

- Technology Steering Committee approval
- Board of Directors approval for major policies (cybersecurity, data governance)
- CEO signature and effective date
- Staff training and acknowledgment (employees sign confirming they've read and understood policies)
- Policies published in Mountain Line's HR system and included in Personnel Policy Manual

Policy Review and Updates:

- **Annual review** by Technology Steering Committee
- **Updates as needed** when regulations change, new technologies are adopted, or incidents reveal policy gaps

- **Version control** maintained by IT Manager with change history documented

Success Metrics:

- **Policy coverage:** 100% of identified technology risk areas have documented policies within 12 months
- **Staff awareness:** 95%+ of employees complete policy training and acknowledgment within 30 days of hire or policy updates
- **Policy compliance:** <5 policy violations per year; violations are addressed through progressive discipline
- **Incident reduction:** 25% reduction in technology incidents caused by policy non-compliance within 24 months

Budget Estimate: \$15-20K (legal review, consultant support for policy development, staff training time)

Objective 3.3: Implement Change Management Framework

Description: Adopt structured change management methodology to increase user adoption, reduce resistance, and ensure technology investments deliver intended benefits.

Change Management Model: Prosci ADKAR Model (industry-leading framework, proven in transit environments)

ADKAR Elements Applied to Mountain Line:

A - Awareness of the need for change

- **Why change?** Communicate business case for technology investments (efficiency gains, better data, improved service, regulatory compliance)
- **Communication channels:** CEO messages, department meetings, email updates, Town Halls, intranet articles
- **Stakeholder mapping:** Identify who is impacted by each technology change (operators, dispatchers, technicians, finance staff, customers)

D - Desire to support and participate in change

- **WIIFM (What's In It For Me):** Frame technology benefits from user perspective (easier workflows, less manual data entry, faster access to information)
- **Address concerns:** One-on-one conversations with resisters, address fears (job security, learning curve, workload)
- **Leadership sponsorship:** Visible CEO and department head support for technology initiatives, not just IT-driven mandates

K - Knowledge of how to change

- **Comprehensive training:** Role-based training (operators, dispatchers, technicians, office staff) before Go-Live
- **Multiple training formats:** Classroom training, hands-on labs, online tutorials, quick reference guides, job aids
- **Train-the-trainer:** Identify power users in each department to provide peer support during rollout
- **Refresher training:** Ongoing training for new hires and when systems are upgraded

A - Ability to implement change

- **Hands-on practice:** Pilot deployments, sandbox environments for practice before production use

- **Performance support:** Helpdesk, super users, vendor support hotlines during Go-Live period
- **Accessibility:** Ensure training accommodates different learning styles, literacy levels, tech comfort levels
- **Remove barriers:** Provide adequate time for training (don't expect staff to learn new systems "on the fly"), address equipment limitations (tablets, connectivity)

R - Reinforcement to sustain change

- **Monitor adoption:** Track system usage, identify non-adopters, intervene with additional support
- **Celebrate successes:** Recognize early adopters, share success stories, highlight efficiency gains
- **Continuous improvement:** Gather user feedback, make system adjustments based on real-world experience
- **Leadership accountability:** Department heads responsible for ensuring their teams adopt new systems, not optional

Change Management Process for Major Technology Projects:

Change management for major technology projects needs to be in line with the organization's broader Project Management process. What follows are factors that should be considered.

Step 1: Change Impact Assessment (Project Initiation Phase)

- Who is affected? How many people? What changes to their jobs?
- Change magnitude: Minor adjustment vs. major workflow transformation?
- Organizational readiness: Is this the only change happening, or change fatigue?
- Risk factors: History of failed technology projects? Tight timeline?

Step 2: Sponsorship Coalition (Planning Phase)

- Identify executive sponsor (usually CEO or a Deputy GM for major projects)
- Engage department heads as change champions
- Clarify sponsor roles: visible support, communications, obstacle removal, accountability

Step 3: Communication Plan (Throughout Project)

- **90-60-30-day campaign** before Go-Live: What's changing, why, when, how to prepare
- **Targeted messages** for different audiences (operators, supervisors, office staff, customers)
- **Two-way communication:** Town Halls with Q&A, suggestion boxes, feedback surveys
- **Consistent messaging:** Coordinate across departments, avoid conflicting information

Step 4: Training Plan (Pre-Go-Live)

- **Training needs analysis:** What do users need to know to do their jobs with new system?
- **Training development:** Curriculum design, materials creation (presentations, videos, manuals)

- **Training delivery:** Schedule training sessions, accommodate shift schedules (operators), provide backfill coverage
- **Training evaluation:** Knowledge checks, hands-on assessments, certification where appropriate

Step 5: Resistance Management (Throughout)

- **Anticipate resistance:** Common sources (fear of job loss, "the old way worked fine," learning curve anxiety)
- **Identify resisters:** Supervisors monitor resistance behaviors (refusal to attend training, workarounds, complaints)
- **Intervention strategies:** One-on-one conversations, address concerns, clarify expectations, involve resisters in solution design
- **Escalation:** Progressive discipline if resistance becomes insubordination (rare, but necessary accountability)

Step 6: Go-Live Support (Implementation Phase)

- **Extra support staffing:** Vendor on-site, super users available, IT helpdesk extended hours
- **Parallel operations:** Run old and new systems simultaneously for transition period when practical
- **Rapid issue resolution:** Daily stand-up meetings to triage problems, escalate to vendor, communicate workarounds
- **Patience and encouragement:** Expect learning curve, celebrate small wins, avoid criticism of mistakes

Step 7: Sustainment and Continuous Improvement (Post-Go-Live)

- **Adoption metrics:** System login rates, feature usage, workarounds vs. intended process
- **User feedback:** Surveys, focus groups, suggestion box, identify enhancement needs
- **System optimization:** Configuration tweaks, add training modules for underused features, remove unnecessary steps
- **Reinforce successes:** Report on benefits achieved (time savings, error reduction, better data quality)

Change Management Roles:

CEO/Executive Sponsor:

- Articulate vision and business case for change
- Visible and active participation (kickoff meetings, Town Halls, Go-Live presence)
- Remove organizational barriers (budget, staffing, policy conflicts)
- Hold department heads accountable for adoption in their areas

Deputy GM/Change Management Lead:

- Overall change management strategy and execution
- Coordinate communication, training, and resistance management activities
- Monitor adoption metrics and intervene where needed
- Report to Technology Steering Committee on change readiness

IT Manager:

- Project management for IT specific systems implementation
- Coordinate training content development with vendor support
- Helpdesk and user support coordination
- Oversee system configuration based on user feedback

Department Heads (Operations, Fleet, Maintenance, Finance, HR):

- Project management for systems implemented within their department
- Champion change within their departments
- Identify super users and change advocates
- Ensure staff attend training
- Monitor adoption and address resistance
- Provide user feedback to improve system

Project Consultants (if applicable):

- Change management methodology and tools
- Communication plan development
- Training program design
- Lessons learned documentation and continuous improvement

Success Metrics:

- **User adoption:** 90%+ of users actively using new systems within 30 days of Go-Live
- **Training completion:** 100% of affected staff complete required training before Go-Live
- **Go-Live success:** System available for use on day 1 with <10% of users requiring additional support beyond standard helpdesk
- **Benefit realization:** Achieve 75%+ of projected benefits (time savings, error reduction, etc.) within 12 months
- **User satisfaction:** 4.0+ rating (out of 5.0) on post-implementation survey

Budget Estimate: \$25-50K per major project (consultant support, training materials, staff time for training delivery, communication campaigns)

Objective 3.4: Develop Business Continuity and Disaster Recovery Plan

Description: Document procedures to maintain essential transit operations and restore IT systems following disruptive events (cyberattacks, natural disasters, equipment failures, pandemics).

Business Continuity Plan (BCP) vs. Disaster Recovery Plan (DRP):

Business Continuity Plan: Focuses on continuing **essential business functions** during disruption

- How to operate buses during technology outage (manual dispatch, paper manifests, radio communications)

- How to process payroll if financial system is down
- How to maintain safety and security without camera systems

Disaster Recovery Plan: Focuses on **restoring IT systems and data** after disruption

- Steps to rebuild servers, restore from backups, bring systems online
- Technology-specific procedures, RTO/RPO objectives
- Vendors contact information for emergency support

Both plans are complementary and should be developed together.

Critical Business Functions (Mountain Line):

Tier 1 - Essential (must continue during any disruption):

- **Fixed-route bus service:** Core mission, public depends on service for work/medical/school trips
- **Paratransit service:** ADA-required, critical for disabled community
- **Dispatch communications:** Safety-critical, must communicate with operators
- **Facility access:** Secure access to Kaspar Drive and DCC facilities
- **Safety/security monitoring:** Basic capability to respond to emergencies

Tier 2 - Important (resume within 24-48 hours):

- **Financial operations:** Payroll processing, accounts payable, grant invoicing
- **Maintenance dispatch:** Work order management, parts ordering
- **Customer service:** Phone/email support, complaint handling
- **HR functions:** Time and attendance, benefit administration

Tier 3 - Supporting (resume within 1 week):

- **Planning and analysis:** Service planning, performance reporting
- **Marketing and communications:** Website updates, social media, promotions
- **Administrative functions:** Procurement, contract management, records management

IT Systems Recovery Priorities:

System	Criticality	RTO (Recovery Time Objective)	RPO (Recovery Point Objective)
GMV CAD/AVL	Critical	4 hours	1 hour
Dispatch radio	Critical	1 hour	N/A (voice only)

System	Criticality	RTO (Recovery Time Objective)	RPO (Recovery Point Objective)
Network/internet connectivity	Critical	4 hours	N/A
Email (Microsoft 365)	High	8 hours	1 hour
Financial system (Sage/RAMP)	High	24 hours	24 hours (daily backups acceptable)
Fare collection system	High	24 hours	1 hour (transaction data)
Fleet management system	Medium	48 hours	24 hours
HR system	Medium	72 hours	24 hours
Security cameras (live)	High	8 hours	N/A (live feed, recorded video less time-sensitive)
Facilities access control	High	8 hours	1 hour (log data)

Disaster Scenarios and Response:

Scenario 1: Ransomware Attack

- **Indicators:** Files encrypted, ransom note displayed, systems locked
- **Immediate response:**
 - Isolate infected systems from network (disconnect network cables, disable Wi-Fi)
 - Contact cybersecurity support (ADOT/DHS, IT Manager, CEO)
 - Report to CISA within 24 hours per TSA Security Directive
 - Do NOT pay ransom (FBI/CISA guidance, no guarantee of decryption, funds criminal enterprise)
- **Recovery:**
 - Assess extent of encryption (which systems, which backups are clean)
 - Restore from most recent clean backups
 - Rebuild infected systems from scratch (reimage, don't trust "cleaned" systems)

- Implement additional security controls to prevent re-infection
- **Business continuity:** Revert to manual operations (paper manifests, radio dispatch) until systems restored

Scenario 2: Facility Fire/Flood (Kaspar Drive Operations Center)

- **Indicators:** Fire alarm, water damage, facility evacuation
- **Immediate response:**
 - Ensure personnel safety (evacuation, accounting for all staff)
 - Contact emergency services (fire, police, utilities)
 - Activate alternate operations location (Downtown Connection Center as backup dispatch)
- **Recovery:**
 - Assess facility damage and estimated restoration time
 - Relocate critical operations to DCC (dispatch, maintenance coordination)
 - Reroute IT network traffic to DCC (if Kaspar fiber cut, rely on cellular internet, VPN)
 - Procure temporary office trailers if needed for extended displacement
- **Business continuity:** Operate dispatch from DCC, temporarily reduce maintenance capacity

Scenario 3: Extended Internet/Network Outage

- **Indicators:** Loss of connectivity to cloud systems (Email, CAD/AVL, etc.)
- **Immediate response:**
 - Determine scope (entire facility, ISP failure, upstream provider, etc.)
 - Contact provider for estimated restoration time
 - Activate backup connectivity if available (cellular hotspots, backup ISP circuit)
- **Recovery:**
 - Monitor ISP restoration progress
 - If extended outage (>4 hours), transition to contingency operations
 - Catch up data entry when systems restored (batch upload trip data, work orders, etc.)
- **Business continuity:** CAD/AVL may have offline mode (store data locally, sync when connectivity restored), dispatch uses radio and mobile phones for operator communications

Scenario 4: Pandemic/Public Health Emergency (COVID-19 lessons learned)

- **Indicators:** Health authority orders, employee illness, public fear of transit
- **Immediate response:**
 - Follow health authority guidance (masks, distancing, cleaning protocols)

- Enable remote work for office staff (VPN access, laptops, Microsoft Teams)
- Adjust service levels if operator availability is low
- **Recovery:**
 - Gradual return to normal operations as health conditions improve
 - Maintain enhanced cleaning and safety protocols
 - Monitor ridership recovery and adjust service accordingly
- **Business continuity:** Essential operations continue (drivers, dispatchers, maintenance), administrative staff work remotely

Plan Development and Maintenance:

Phase 1: BCP/DRP Development (Months 1-6)

- Conduct Business Impact Analysis (BIA) - identify critical functions, dependencies, tolerable downtime
- Document current backup and recovery capabilities (inventory what exists today)
- Identify gaps (systems without backups, missing recovery procedures, no alternate work locations)
- Write BCP and DRP documents with step-by-step procedures
- Identify key personnel roles and 24/7 contact information

Phase 2: Testing and Validation (Months 7-12)

- **Tabletop exercises:** Walk through disaster scenarios with management team, identify gaps in plans
- **Technical recovery tests:** Restore systems from backups, verify RTO/RPO targets are achievable
- **Functional exercises:** Simulate disruption (e.g., "the dispatch center is unavailable"), actually operate from alternate location

Phase 3: Annual Maintenance (Ongoing)

- **Annual review:** Update BCP/DRP
- **Update contact lists:** Staff changes, vendor support numbers, emergency services
- **Incorporate lessons learned:** Real incidents or exercises reveal plan weaknesses
- **Annual testing:** Minimum one exercise per year (alternate tabletop and functional drills)

Alignment with Regional Plans:

- **City of Flagstaff Emergency Operations Plan:** Coordinate Mountain Line's role during community-wide emergencies
- **Coconino County Emergency Management:** Participate in county-wide exercises and emergency operations center (EOC) activation
- **NAU:** Campus plan

- **Arizona Department of Transportation:** Coordinate on statewide transportation disruptions (I-40 closures, wildfire evacuations)

Success Metrics:

- **Plan completion:** BCP and DRP fully documented and approved by Board within 12 months
- **Staff preparedness:** 90%+ of key personnel know their BCP/DRP roles and can execute during drill
- **Recovery capability:** Achieve RTO targets in testing (restoring critical systems within defined timeframes)
- **Incident performance:** When real incidents occur, BCP/DRP followed and Post-Incident Review identifies continuous improvement opportunities

Budget Estimate: \$30-50K (consultant support for BIA and plan development, testing exercises, staff training, backup infrastructure improvements)

Goal 4: Infrastructure & Operations Excellence

Strategic Objective: Modernize IT infrastructure, strengthen cybersecurity posture, and establish sustainable service desk capabilities to support reliable, secure, and efficient technology operations.

Objective 4.1: Modernize Network and Infrastructure

Description: Maintain network equipment, expand connectivity between facilities, and migrate to cloud-based infrastructure where appropriate to improve reliability, scalability, and manageability.

Current State Assessment:

- **Two-facility operations:** Kaspar Drive headquarters and Downtown Connection Center (DCC)
- **Cloud adoption:** Partial cloud-hosted systems, but many on-premises systems
- **Backup/redundancy:** Cellular backup at both locations, automatic cutover. Single points of failure: no access to on-premises servers during point-to-point outage.

Infrastructure Modernization Components:

1. Inter-Facility Connectivity

Requirements:

- **High bandwidth:** Support vehicle video uploads (camera systems), CAD/AVL data, voice communications
- **Monitoring:** New REI video system implementation requires monitoring of bandwidth to ensure sufficient capacity and quality
- **Low latency:** CAD/AVL dispatch requires minimal delay
- **High reliability:** 99.9%+ uptime (8.76 hours downtime per year acceptable maximum)
- **Redundancy:** Backup connectivity path if primary link fails

Analysis of Options:

Option A: Dedicated Fiber (Existing)

- **Pros:** Highest bandwidth (1-10 Gbps), lowest latency, most reliable, private network (security)

- **Cons:** Higher upfront cost (fiber installation if not existing), geographic limitations
- **Cost:** \$500-1,500/month recurring

Option B: Metro Ethernet (Business-class internet with QoS)

- **Pros:** Lower cost than fiber, adequate bandwidth (100 Mbps-1 Gbps), good reliability
- **Cons:** Shared infrastructure (internet service provider congestion possible), less secure than private fiber
- **Cost:** \$300-800/month recurring

Option C: City Fiber (Not currently available)

Recommendation: Maintain existing dedicated fiber as primary link between Kaspar and DCC, increasing bandwidth as necessary and add Metro Ethernet or City fiber as a backup when available.

2. Network Equipment Refresh

Current Equipment Assessment: Conduct inventory of network switches, routers, wireless access points, firewalls

- **Age:** Equipment >7 years old should be replaced (end-of-support risk, performance limitations)
- **Capacity:** Does current equipment support bandwidth needs (EV charging data, video streaming, CAD/AVL)?
- **Security features:** Modern firewalls with intrusion prevention, wireless with WPA3 encryption

Refresh Strategy:

- **Core switches** (data center): Enterprise-grade, stackable, 10 Gbps uplinks, redundant power supplies
- **Distribution switches** (wiring closets): Gigabit ports, PoE+ for VoIP phones and wireless APs
- **Wireless access points:** Modern 802.11ax (Wi-Fi 6 or higher), high density support (DCC public areas), guest network segregation
- **Firewalls:** Next-generation firewalls (NGFW) with intrusion prevention, VPN, SSL inspection, application control
- **Lifecycle plan:** 5-7 year replacement cycle, budget 20% of equipment annually to avoid "rip and replace" every 7 years

Budget Estimate: \$75-125K (equipment), \$15-25K (installation and configuration)

3. Cloud Migration Strategy

Cloud-First Principle: New systems should be cloud-based unless compelling reason for on-premises (reduce server hardware, improve accessibility, leverage vendor expertise)

Cloud Adoption Roadmap:

Already Cloud (maintain):

- Microsoft 365 (email, OneDrive, Teams, SharePoint)
- CAD/AVL (cloud SaaS)
- Credit card processing (cloud)
- Fleet management system (cloud SaaS)

- HR system (cloud SaaS)
- Fare collection system (cloud SaaS)

Migrate to Cloud (priorities):

- **Data warehouse** - cloud-native data platforms
- **Backup and disaster recovery** - offsite cloud storage
- **File shares**

Remain On-Premises (justified reasons):

- **Security camera DVRs:** Local storage for high-bandwidth video, cloud upload for sharing only
- **Legacy systems:** If replacement is not yet funded, maintain on premises until EOL

Cloud Benefits:

- **Reduced capital costs:** No server hardware purchases, vendor hosts infrastructure
- **Scalability:** Easily add users, storage, and computing capacity as agency grows
- **Accessibility:** Remote work enabled, access from multiple facilities, mobile access
- **Reliability:** Vendor SLAs typically 99.9-99.99% uptime (better than small agency can achieve with limited IT staff)
- **Security:** Vendors have dedicated security teams, 24/7 monitoring, compliance certifications (FedRAMP, SOC 2)
- **Disaster recovery:** Geographic redundancy built-in, backups automated

Cloud Risks and Mitigation:

- **Vendor lock-in:** Choose vendors with data export capabilities, avoid proprietary formats
- **Internet dependency:** Requires reliable internet (addressed in connectivity objective above)
- **Data sovereignty:** FTA-funded data must remain in U.S. (specify in contracts)
- **Cost management:** Monitor cloud spending, avoid over-provisioning, right-size resources

Budget Estimate: Cloud migration is primarily shift from capital (servers) to operating expense (subscriptions). Annual cloud costs are estimated in individual system objectives (data warehouse, backup and disaster recovery, file shares).

4. Server and Storage Infrastructure

For Remaining On-Premises Systems:

- **Virtualization:** Continue using virtual machines (VMs) to consolidate servers (reduce hardware, improve utilization)
- **Storage area network (SAN):** Centralized storage for VMs, automatic backup integration
- **Server refresh:** 5-year replacement cycle for physical hosts
- **Capacity planning:** Monitor storage growth (video, data warehouse archives), add capacity before running out

Budget Estimate: \$50-75K per 5-year refresh cycle (physical servers, storage expansion, virtual host licensing)

Implementation Timeline:

- **Months 1-3:** Network assessment, equipment inventory, connectivity evaluation between Kaspar and DCC
- **Months 4-6:** Failover testing
- **Months 7-12:** Network equipment refresh (phased rollout, start with oldest equipment)
- **Ongoing:** Cloud migration occurs project-by-project as systems are replaced (data warehouse, backup and disaster recovery, file shares)

Success Metrics:

- **Network uptime:** 99.9%+ availability (monitored by network management system)
- **Inter-facility connectivity:** <5ms latency, >500 Mbps bandwidth, <1 hour outage per year
- **Cloud adoption:** 95% of applications cloud-based by Year 5
- **Equipment age:** No network equipment >7 years old by Year 3

Objective 4.2: Strengthen Cybersecurity Posture

Description: Mature from reactive to proactive cybersecurity, comply with TSA Security Directive 1580-21-01, CIS Controls, and NIST Cybersecurity Framework, and protect against growing threats targeting transit agencies.

Current State: Needs assessment identified "reactionary" security posture, lack of documentation of cybersecurity plans.

Target State: NIST Cybersecurity Framework Maturity Level 3 (Managed) by Year 3, Level 4 (Adaptive) by Year 5

Cybersecurity Improvement Roadmap:

1. TSA Security Directive Compliance (IMMEDIATE PRIORITY - Year 1)

TSA Security Directive 1580-21-01 (December 2021) requires transit agencies to:

Requirement 1: Designate Cybersecurity Coordinator

- **Action:** IT Manager designated as Cybersecurity Coordinator ("CyberCoord")
- **Responsibilities:** Cybersecurity strategy, incident response coordination, TSA liaison, Board/CEO reporting
- **Documentation:** Designation letter on file, contact information reported to TSA/CISA
- **Timeline:** Completed as of January 1st, 2026.

Requirement 2: Report Cybersecurity Incidents to CISA

- **Action:** Document incident reporting procedure, 24-hour notification requirement
- **Covered incidents:** Ransomware, data breach, operational technology disruption, attempted intrusions
- **Reporting method:** CISA Central reporting portal, follow-up phone call for significant incidents
- **Timeline:** Procedure documented and staff trained (Months 1-2)

Requirement 3: Complete Cybersecurity Vulnerability Assessment

- **Action:** Conduct comprehensive assessment of IT and OT systems
- **Scope:** Network, servers, operational technology (CAD/AVL, fare system, security cameras, access control), security policies, staff awareness
- **Method:** Self-assessment using APTA OT-CMF or FTA Cybersecurity Assessment Tool for Transit (CATT), and/or external penetration test
- **Timeline:** Complete assessment by Month 6, repeat annually

Requirement 4: Develop Cybersecurity Incident Response Plan

- **Action:** Document procedures for detecting, responding to, and recovering from cyber incidents (see Objective 3.4 BCP/DRP)
- **Elements:** Incident classification, escalation procedures, containment actions, communication plan, recovery steps, lessons learned
- **Testing:** Annual tabletop exercise
- **Timeline:** Plan documented by Month 9, tested by Month 12

2. NIST Cybersecurity Framework Implementation (Year 1-5)

NIST CSF 2.0 Core Functions:

GOVERN (Foundation - Year 1-2):

- **Establish cybersecurity governance:** Technology Steering Committee oversees cybersecurity strategy
- **Document policies:** Cybersecurity policy, acceptable use policy, incident response plan (Objective 3.2)
- **Risk management:** Conduct annual risk assessments, prioritize threats, allocate budget to highest risks
- **Third-party risk:** Assess vendor cybersecurity (require SOC 2 reports, insurance, breach notification clauses in contracts)
- **Workforce development:** Cybersecurity training for IT department (industry standard training and certifications), awareness training for all staff

IDENTIFY (Know Your Assets - Year 1-2):

- **Asset inventory:** Document all IT and OT systems, software, data repositories (extend current system inventory)
- **Network mapping:** Diagram network architecture, identify trust boundaries, document connections to internet and between facilities
- **Data classification:** Identify sensitive data (PII, financial, operational), where it's stored, who has access
- **Threat intelligence:** Subscribe to transit sector threat feeds (PT-ISAC - Public Transportation Information Sharing and Analysis Center)

PROTECT (Safeguards - Year 1-3):

- **Access controls:** Enforce MFA for remote access and privileged accounts, role-based access, least privilege principle

- **Endpoint protection:** Maintain current antivirus and patch management, enable Windows Defender cloud and local workstation management
- **Network security:** Segment networks (operations/OT separate from office IT, guest Wi-Fi isolated), intrusion prevention system (IPS)
- **Data protection:** Encryption for sensitive data at rest and in transit, backup encryption, secure data disposal
- **Security awareness training:** Bi-monthly mandatory refresher training, phishing simulations monthly, security reminders (posters, intranet)

DETECT (Find Threats Early - Year 1-3):

- **Security monitoring:** Implement Security Information and Event Management (SIEM) system to aggregate logs from firewalls, servers, applications, detect anomalies
- **Intrusion detection:** Network and host-based intrusion detection systems (IDS/IPS)
- **Vulnerability scanning:** Quarterly automated scans of network and systems, prioritize patching based on results
- **Audit logging:** Enable logging on all critical systems, retain logs 1 year minimum for forensic investigation
- **Threat hunting:** Proactive searches for indicators of compromise (IOCs), leveraging PT-ISAC threat intelligence

RESPOND (React Quickly - Year 1-4):

- **Incident response plan:** Documented and tested (Objective 3.4)
- **Incident response team:** IT Manager, CEO, Deputy GM of Operations, external support (AZNG, DHS, FBI cyber task force if needed)
- **Communication plan:** Internal (staff, Board), external (FTA, TSA, CISA, public if data breach), media relations
- **Containment procedures:** Isolate compromised systems, preserve evidence, prevent spread
- **Forensic analysis:** Determine root cause, extent of compromise, data exfiltrated

RECOVER (Restore Operations - Year 3-5):

- **Disaster recovery plan:** Documented and tested (Objective 3.4)
- **Backup restoration:** Restore systems from clean backups, verify integrity before returning to service
- **Lessons learned:** Post-incident review, identify improvements to prevent recurrence
- **Communications:** Notify stakeholders when operations restored, transparency about incident and corrective actions

3. Operational Technology (OT) Security (Year 2-4)

Transit-specific challenges: Secure operational technology systems (CAD/AVL, fare validators, security cameras, EV chargers, mobile routers) that were often deployed without cybersecurity considerations. Other non-transit-specific systems (ex: HVAC, access systems, UPS) are covered as well.

OT Security Best Practices:

- **Network segmentation:** Separate OT network from IT network, air-gap if possible, strict firewall rules between them

- **Vendor remote access:** VPNs with MFA for vendor support, time-limited access, monitor vendor activity
- **Change management:** Test OT system updates in lab before production deployment, schedule maintenance windows
- **Anomaly detection:** Baseline normal OT network traffic, alert on deviations (could indicate malware or unauthorized access)
- **Legacy system risk:** Accept risk for un-patchable legacy systems, compensate with network isolation, plan replacement

4. Security Tools and Services (Year 1-5)

Current Tools (maintain and optimize):

- **CrowdStrike:** Endpoint detection and response (EDR), provided by AZDoHS - ensure deployed on all workstations, laptops, servers
- **Tanium:** Patch management and endpoint visibility, provided by AZDoHS. Leverage for vulnerability management

Additional Tools (evaluate and procure):

- **Multi-Factor Authentication (MFA):** deploy for remote access, privileged accounts - Year 1 Evaluate to ensure Microsoft is still appropriate solution
- **Security Information and Event Management (SIEM):** Azure Sentinel (cloud), Splunk, or similar - aggregate logs, detect threats - Year 2-3, **\$15-30K annually**
- **Vulnerability scanner:** Evaluate to ensure Tanium is still appropriate solution; otherwise look at Tenable Nessus, Qualys, or similar - quarterly scans - Year 2, **\$5-10K annually**
- **Phishing simulation:** Evaluate to ensure KnowBe4 is still appropriate solution: Proofpoint, or similar - test staff, targeted training - Year 2, **\$3-5K annually**
- **Backup and recovery:** offsite encrypted backups - Year 1, **\$10-20K annually**

5. Cybersecurity Staffing and Training

IT Manager Bench Strength Cybersecurity Training and Certification (Year 1-2):

- **Target:** CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), GIAC (SANS Institute), or similar certifications
- **Benefits:** Industry-recognized credential, demonstrates competency, professional development
- **Cost:** \$3-5K (exam fees, study materials, training course)
- **Time commitment:** 3-6 months study, 1 week training course

Staff Security Awareness Training (Ongoing):

- **All staff bi-monthly training:** Cybersecurity basics, phishing identification, password security, incident reporting - 10-15 minutes online course
- **Targeted training:** IT staff (advanced technical training), finance (wire fraud prevention), HR (social engineering awareness)
- **Phishing simulations:** Monthly tests, employees who click malicious links receive just-in-time remedial training

External Support (as needed):

- **Penetration testing:** Annual external pen test to identify vulnerabilities - \$15-25K or sponsored
- **Incident response retainer:** Pre-contract with cybersecurity firm for rapid response if major incident - \$5-10K annual retainer
- **vCISO (Virtual Chief Information Security Officer):** Fractional CISO services for strategic guidance - \$2-5K monthly (consider Year 4-5 if budget allows)

Implementation Timeline:

- **Year 1 (Months 1-12):** TSA compliance (Coordinator, reporting procedure, assessment, IR plan), MFA deployment, backup improvements, IT Manager training
- **Year 2 (Months 13-24):** SIEM implementation, vulnerability scanning, phishing simulations, network segmentation (OT from IT), IT Manager training
- **Year 3 (Months 25-36):** Advanced threat detection, penetration testing, OT security hardening, audit and refine
- **Year 4-5 (Months 37-60):** Mature to NIST CSF Level 4 (Adaptive), continuous improvement, automation

Success Metrics:

- **TSA compliance:** 100% compliance with Security Directive 1580-21-01 requirements by Month 12
- **NIST CSF maturity:** Progress from Level 2 (Initial) to Level 3 (Managed) by Year 3, Level 4 (Adaptive) by Year 5
- **Incident reduction:** 50% reduction in or 2% or less ongoing successful phishing attacks (measured by click rate on simulations)
- **Patching compliance:** 95%+ critical/high-risk patches deployed within defined timeframes (15/30 days)
- **Staff awareness:** 100%+ pass bi-monthly security awareness training assessment
- **Zero ransomware:** No successful ransomware attacks (due to prevention, early detection, and rapid response)

Budget Estimate:

- **Year 1:** \$40-60K (TSA compliance, MFA, backup improvements, IT Manager training/certification)
- **Year 2:** \$50-75K (SIEM, vulnerability scanning, phishing simulation, network segmentation equipment)
- **Year 3:** \$30-50K (penetration testing, OT security improvements, ongoing tool subscriptions)
- **Year 4-5:** \$30-40K annually (ongoing subscriptions, annual pen test, training, continuous improvement)
- **Total 5-year investment:** \$180-265K

Objective 4.3: Establish Sustainable IT Support Model

Description: Fill critical IT staffing gaps, implement IT service management (ITSM) processes, and strengthen service desk to provide responsive, professional support to Mountain Line staff.

Current State Challenges:

- **IT Department Bench Strength:** department bench strength and succession planning are the biggest threat and priority to the department in areas from strategy to helpdesk to unsustainable workloads
- **Data Analyst position needed:** Gap for data warehouse implementation and BI
- **IT Technician position needed:** Needed for day-to-day operational helpdesk, desktop support, vehicle technology troubleshooting, and equipment maintenance
- **Support ticketing system compliance:** Occasional requests come via email, phone, walk-up - difficult to track, prioritize, measure

Target State:

- **Right-sized IT team:** 4.5 FTEs (IT Manager, Systems Administrator, IT Specialist, IT Technician, Document Control Specialist) for a 100+-employee, 7 day-a-week transit agency spread across two locations
- **Structured ITIL-compliant service desk:** Ticketing system, defined SLAs, performance metrics
- **Proactive support:** Regular maintenance, system monitoring, user training vs. reactive firefighting

Staffing Strategy:

IT Manager (existing position):

- **Strategic focus:** Technology planning, vendor management, project management, cybersecurity
- **Freed from:** Day-to-day helpdesk tickets, routine desktop support, basic troubleshooting
- **Time allocation:** 50% strategy/projects, 40% operations/vendor management, 10% escalated support

IT Technician (NEW POSITION - HIGH PRIORITY):

- **Primary responsibilities:**
 - Service desk (phone, email, in-person support requests)
 - Desktop/laptop support (Windows troubleshooting, software installation, hardware repairs)
 - Mobile device support (tablets for operators/technicians, smartphones)
 - Account administration (Microsoft 365, Active Directory user accounts, password resets)
 - Equipment maintenance (printers, monitors, peripherals, conference room AV)
 - New employee technology onboarding (equipment setup, account creation, training)
 - Asset inventory management (track equipment, software licenses, warranties)
 - Transit technology support and maintenance (Works closely with IT Specialist, Systems Administrator, and Fleet Department)
- **Qualifications:** This is intended as an entry level position to provide a pipeline for higher level IT positions. Associate degree preferred, or equivalent experience or technical certifications (CompTIA A+, Network+, Microsoft, etc.); customer service skills; driver's license (travel between Kaspar and DCC facilities)
- **Salary range:** \$45-55K annually + benefits (~40%) = \$63-77K (entry level, Arizona market)

- **Reporting:** Reports to IT Manager

Data Analyst (new position):

- **Primary responsibilities:**
 - Data warehouse administration (ETL job monitoring, data quality, user support)
 - Business intelligence report/dashboard development (Power BI, Tableau)
 - Data analysis for grant applications, Board reports, performance measurement
 - Support planning department with ridership analysis, service optimization, NTD reporting
 - Note: these duties are largely handled by the Strategic Performance Planner currently; hiring of a dedicated Data Analyst is a long-term goal
- **Qualifications:** Bachelor's in Data Analytics, Business Intelligence, Statistics, or related field; 2+ years experience with SQL, data visualization tools (Power BI/Tableau); transit experience preferred but not required
- **Salary range:** \$65-80K annually + benefits (~40%) = \$91-112K (small agency, Arizona market, mid-level position)
- **Reporting:** Reports to Planning Director

Hiring Timeline:

- **IT Technician:** Priority 1 - hire by Month 12 (immediate relief for IT team, improves user support)
- **Data Analyst:** Priority 2 - hire when workload dictates a dedicated position (enables data warehouse implementation to proceed)

Recruiting Strategy:

- **IT Technician:** Local Flagstaff candidates, NAU or CCC information systems/IT program graduates. Offers career advancement opportunity (small team, diverse responsibilities, potential succession path)
- **Data Analyst:** Regional candidates (Flagstaff, Phoenix metro willing to relocate), highlight interesting transit analytics work, downtown location, mission-driven organization

Retention Strategy:

- **Competitive compensation:** Benchmark salaries to comparable transit agencies and other Flagstaff local government agencies
- **Professional development:** Support certifications, training, conference attendance (APTA conferences, etc.)
- **Work-life balance:** Reasonable on-call expectations, flex schedule when possible
- **Meaningful work:** Emphasize mission (public service, community mobility, sustainability) vs. corporate IT

IT Service Management (ITSM) Implementation:

IT Service Desk Platform:

- **Requirements:** Ticketing system, asset management, knowledge base, SLA tracking, reporting

Service Desk Processes:

Ticket Lifecycle:

1. **Submission:** User submits ticket via email, web form, phone
2. **Triage:** IT Technician assesses urgency/impact, assigns priority (P1-P4), attempts initial resolution
3. **Assignment:** If escalation needed, assign to IT Manager or vendor (e.g., network issue, server problem)
4. **Resolution:** Fix applied, tested, documented in ticket
5. **Closure:** User notified, confirms issue resolved, ticket closed
6. **Follow-up:** Quarterly review closed tickets, identify recurring issues, proactive fixes

Priority Levels and SLAs: (Note: Response and Resolution Times are business hours/days.)

Priority	Definition	Response Time	Resolution Time	Examples
P1 - Urgent	Service outage, many users impacted, operations stopped	2 Hours	1 day	Critical outage or issue preventing essential business functions. Ex: CAD/AVL down, network outage, email down.
P2 - High	Significant degradation, key users impacted	4 hours	3 days	Individual workstation crash, printer down, slow performance. Disruption, but workaround exists.
P3 - Medium	Minor issue, workaround available	6 hours	7 days	Software glitch, non-urgent but affects productivity.
P4 - Low	Informational, no urgency	8 hours	30 days	How-to questions, non-urgent enhancement requests, minor inconveniences.

Service Catalog (define what IT supports):

- **Supported:** Windows workstations/laptops, Microsoft 365 apps, business software (Sage, GMV, RTA, Optibus, etc.), vehicle diagnostic software, printers, network connectivity, mobile devices (agency-provided), conference room AV, vehicle technology (routers, camera systems, fare and CAD/AVL equipment), customer-facing applications (fare collection, rider apps)
- **Limited support:** Personal devices (BYOD) - basic troubleshooting only, no data recovery or repairs
- **Not supported:** Personal software (games, non-business apps), personal cloud storage (Dropbox, iCloud), unauthorized hardware

Knowledge Base:

- **Self-service articles:** Common how-to articles (self-password reset, VPN setup, printer connection, mobile app installation)
- **Internal documentation:** System configurations, vendor contacts, troubleshooting guides for IT staff

- **Video tutorials:** Screen recordings for complex procedures (better than written docs for some users)

User Communication:

- **Ticket confirmation:** Auto-email when ticket submitted (reassurance, ticket number for reference)
- **Status updates:** IT Technician updates ticket and emails user at milestones (assigned to technician, vendor engaged, parts ordered, etc.)
- **Outage notifications:** Proactive emails for planned maintenance or known outages (CAD/AVL upgrade, network maintenance window)
- **IT newsletter:** Quarterly tips, security reminders, new features, upcoming changes

Success Metrics:

- **User satisfaction:** Quarterly survey, target 4.0+ out of 5.0 rating on IT support responsiveness and quality
- **SLA compliance:** 90%+ of tickets meet response time and resolution targets
- **First-call resolution:** 70%+ of tickets resolved by IT Technician without escalation
- **Ticket volume trends:** Monitor for increases (may indicate training needs, system problems, staffing inadequacy)
- **Mean time to resolve (MTTR):** Track average resolution time by priority, trend should decrease as processes mature

Budget Estimate:

- **IT Technician salary:** \$45-55K annually + benefits (~40%) = \$63-77K
- **Data Analyst salary:** \$65-80K annually + benefits (~40%) = \$91-112K
- **ITSM platform:** \$5-10K annually
- **Onboarding costs:** \$10-15K (workstations, monitors, software licenses, training, recruitment)
- **Total Year 1:** \$65-82K (pro-rated if IT Technician hired mid-year)
- **Years 2-5:** \$169-214K annually (ongoing salaries and ITSM subscription)

Goal 5: Security, Compliance & Risk Management

Strategic Objective: Enhance rider experience through improved real-time information access, modern mobile ticketing, and data-driven service planning that makes Mountain Line the first choice for mobility in Flagstaff.

Objective 5.1: Data-Driven Service Planning and Performance Measurement

Priority: MEDIUM (depends on data warehouse completion)

Description: Leverage integrated data systems to provide the Planning and Operations departments with the tools needed to continuously optimize service based on ridership patterns, operational performance, and customer feedback.

Service Planning Applications:

1. Route Optimization

Current Limitation: Service adjustments historically based on complaints and management intuition vs. data

Data-Driven Approach:

- **Ridership patterns:** Analyze APC data (boarding/alighting by stop, time of day, day of week)
- **Route performance:** Compare routes on metrics (cost per passenger, ridership trends, OTP, revenue per mile)
- **Travel demand:** Where do riders actually want to go (origin/destination pairs from fare system, APC data)?
- **Service efficiency:** Which routes have low ridership but high cost? Which routes are overcrowded?

Tools and Process:

- **Route optimization:** software showing ridership patterns, suggesting service modifications
- **Data analysis:** Conduct annual review before next fiscal year budget planning
- **Stakeholder engagement:** gather community input, present findings to TAC/Board

Example Analysis:

- "Route 3 has 15% lower ridership on Sundays despite same frequency as weekdays. Reducing Sunday frequency from every 30 to every 45 minutes would save \$50K annually with minimal ridership impact."
- "Route 5 has high demand at 7-8 AM but low afternoon ridership. Shifting a bus from afternoon local service to morning Route 5 would improve system efficiency."

Expected Outcome: 5%+ improvement in cost per passenger through service adjustments aligned with actual demand

2. Service Reliability Monitoring

Current Limitation: OTP tracked but limited visibility into root causes (mechanical, traffic, scheduling, driver performance)

Enhanced Monitoring:

- **Real-time dashboards:** Visibility into current day OTP by route, identify problem routes/times
- **Root cause analysis:** CAD/AVL data shows actual vs. scheduled times, can identify if delay is before/after specific stop (traffic congestion vs. operator spacing issue)
- **Targeted interventions:** If route consistently late, adjust schedule, increase frequency, or address dispatcher/operator practices
- **Accountability:** Track individual operator OTP, provide coaching for consistent offenders

System Requirements:

- **Data warehouse integration:** Link CAD/AVL, schedule data, road network geometry
- **Analytics:** BI dashboards showing daily/weekly/monthly trends
- **Alerts:** Automated alerts when OTP drops below threshold (e.g., <85%)

Example Dashboard:

- Route 7 OTP by day of week: Mon 89%, Tue 87%, Wed 91%, Thu 88%, Fri 84%
- Investigation: Friday low OTP correlates with downtown congestion 4-6 PM

- **Recommendation:** Increase headway on Route 7 during Friday peak (add 1 bus), adjust schedule to reflect realistic running times, or coordinate with city on traffic management

3. Customer Feedback Integration

Channels:

- **In-app ratings:** After each trip, rate experience (satisfaction survey)
- **Web form:** Feedback/complaint submission on website
- **Social media monitoring:** Track mentions on Facebook, Twitter, online reviews
- **Community meetings:** Quarterly TAC and Board discussion of service issues
- **Accessibility feedback:** Specific outreach to riders with disabilities, older adults, LEP communities

Analysis:

- **Trend identification:** Common complaints (e.g., "Buses always late on Route 5", "Drivers rude", "Need route to hospital")
- **Comparison with data:** Does "Route 5 always late" match actual OTP data? If yes, address root cause. If no, communicate why (perception vs. reality).
- **Action tracking:** Each complaint receives response, tracked to resolution or close-out

Implementation:

- **Designated staff:** Customer Service Coordinator manages feedback system, tracks issues, closes loops
- **System:** Integrate with ITSM ticketing system or dedicated customer feedback platform (Zendesk, Freshdesk)

4. Paratransit Performance Optimization

Current State: Paratransit operates separately from fixed route (different technologies, limited integration)

Data Insights:

- **Reservation trends:** When do paratransit riders book? (peak days/times)
- **No-show analysis:** Why do some riders book and not use? (reminder calls, booking errors, life changes?)
- **Geographic demand:** Where are main paratransit trip origins/destinations?
- **Cost per trip:** Compare to fixed-route, identify opportunities to shift eligible riders to fixed-route

Example Analysis:

- "40% of paratransit no-shows are on Wednesdays. Implementing reminder SMS/calls on Tuesday evening could reduce no-shows by 30%, save \$25K annually."
- "Paratransit to downtown has doubled since fixed-route frequency increased. Paratransit capacity constraint can be relieved by promoting fixed-route to ADA-eligible riders with education."

Implementation Timeline:

- **Year 2:** Build data warehouse (includes paratransit data from Spare Labs), develop initial dashboards

- **Year 2-3:** Train staff on data tools, conduct pilot analyses and service changes
- **Year 3-5:** Mature data-driven culture, continuous optimization cycle

Success Metrics:

- **Service efficiency:** 10% improvement in cost per passenger within 5 years through data-driven adjustments
- **Customer satisfaction:** Increase overall satisfaction rating from current baseline to 4.0+ (out of 5.0)
- **Data utilization:** 90% of service decisions supported by data analysis (vs. currently mostly intuition)
- **Responsive action:** <30 days from issue identification to corrective action (vs. current 3-6 months)

Budget Estimate: Included in data warehouse and BI tools (Objective 1.1). Additional staffing (data analyst) covers ongoing service optimization work.

Objective 5.2: Accessibility and Equity in Technology

Priority: HIGH (FTA and legal requirements, alignment with Mountain Line's equity commitment)

Description: Ensure technology investments benefit all riders, particularly those who are disabled, low-income, older adults, and limited-English proficient (LEP).

Accessibility Standards and Compliance:

1. Digital Accessibility (Web and Mobile)

Standard: WCAG 2.1 Level AA (Web Content Accessibility Guidelines)

Key Requirements:

- **Screen reader compatibility:** Website and mobile app work with JAWS, NVDA, VoiceOver (tools that allow blind/low-vision users to access digital content)
- **Keyboard navigation:** All functions operable via keyboard (not just mouse)
- **High contrast:** Text readable for low-vision users (minimum 4.5:1 contrast ratio for body text)
- **Captions and transcripts:** Videos include captions for deaf/hard-of-hearing, transcripts available
- **Plain language:** Avoid jargon, clear instructions (benefit low-literacy and ESL users)

Implementation:

- **Remediation:** Fix identified issues (form labels, color contrast, keyboard traps, etc.)
- **Ongoing testing:** Annual accessibility review, especially after website updates or new features
- **Staff training:** Web developers trained on accessibility best practices, accessibility checklist for all new features

2. Fare System Accessibility

Challenges:

- **Ticket validators:** Physical design accessible to wheelchair users? Buttons/screen operable for blind/low-vision riders?

- **Mobile app:** Fare purchase process usable by people with disabilities
- **Reduced fares:** Enrollment process accessible, verification simple and non-stigmatizing (doesn't require showing disability documentation on bus)

Requirements:

- **Validator design:** Compliant with ADA Standards for Accessible Design (buttons reachable, screen readable)
- **Audio feedback:** Validator provides audio confirmation of successful tap (tone sound, verbal message)
- **Retail reload locations:** Service center staff trained to assist riders with disabilities (taking time, accessible counter)
- **Smart card option:** Physical card alternative to phone-based tickets for accessibility

Implementation: Evaluate in fare system RFP (vendor must meet accessibility standards), test with advisory group of disabled riders before system acceptance

3. Language Access (Limited English Proficiency)

Requirement: Title VI of Civil Rights Act requires transit agencies provide information in languages spoken by LEP communities

Current Situation: Mountain Line has Spanish-speaking population (30%+ of Flagstaff), limited Spanish materials/services historically

Actions:

- **Audit current materials:** Identify what's translated to Spanish (website, schedules, announcements, signage, customer forms)
- **Priority translations:**
 - Website (all pages)
 - Route schedules and maps
 - Onboard announcements and displays
 - Rider guides and policies
 - Customer service forms
 - Safety and emergency instructions
- **Methods:**
 - Professional translation (not relying on bilingual staff volunteers)
 - Back-translation review (translated to Spanish, then back to English to verify accuracy)
 - Community review (Spanish speakers from community validate translations are idiomatic)
- **Multilingual staff:** Ensure customer service and supervisory staff include Spanish speakers for phone support, onboard assistance
- **Signage and displays:** Bilingual wayfinding at DCC, Kaspar, major stops

Implementation:

- **Year 1:** Audit, professional translation of priority materials
- **Year 2:** Implement translated materials across website, signage, customer touchpoints
- **Ongoing:** Maintain translations, update when schedules change, add other languages as community composition shifts

Budget Estimate: \$10-15K annually (professional translation services, multilingual staff time)

4. Affordability and Digital Inclusion

Challenge: Digital-first services (mobile ticketing, online scheduling, account-based payments) exclude unbanked, non-smartphone users, low-income riders

Equity Principles:

- **No digital-only services:** Cash payment options must always be available
- **No digital premium:** Don't charge more for non-digital users (e.g., don't force higher price for cash vs. mobile)
- **Retail access points:** Physical locations to buy passes (accept cash, no online account needed)
- **Accessibility of choice:** Offer multiple options (app, smart card, paper tickets, credit/debit cards, cash) so riders choose what works for them

Implementation:

- **Fare system design** (Objective 2.1): Include requirement for cash payment, physical card, and retail reload locations
- **Service center:** Staffing to assist with fare purchases, account setup for those wanting digital access
- **Partnerships:** Convenience stores, libraries, community centers as additional reload locations (reduces access burden)
- **Free or reduced fare program:** Ensure eligibility enrollment accessible to low-income riders (not dependent on online application)

5. Coordinated Mobility Council

Purpose: Seek ongoing feedback from riders with disabilities and other underrepresented groups on technology implementations by working with the current Coordinated Mobility Council.

Technology Risk Assessment and Mitigation

High-Risk Initiatives (most likely to encounter challenges):

Risk 1: Cybersecurity Incident (Ransomware, Data Breach, OT Attack)

Risk Description: Transit agencies face increasing cybersecurity threats (nation-state actors, ransomware gangs). Mountain Line currently has "reactionary" security posture. Incident impact could include service disruption, data breach of rider PII, operational downtime, reputational damage, regulatory fines.

Probability: 40% (Medium) over 5 years

Impact:

- **Revenue disruption:** Fare collection down, unable to collect payment (loss of revenue/revenue recovery)

- **Service disruption:** CAD/AVL down, unable to operate buses safely (dispatch communications compromised)
- **Data breach:** Rider payment card data, personal information exposed (GDPR-like notification requirements)
- **Ransom demand:** Attackers encrypt data, demand payment (\$100K-\$1M+ depending on organization size)
- **Regulatory penalty:** FTA/TSA investigation, potential loss of federal funding
- **Public trust:** Media coverage, reputation damage, ridership decline

Mitigation Strategies:

Strategy	Responsible
Cybersecurity Coordinator designation (IT Manager) with executive authority	CEO, IT Manager
TSA Security Directive 1580-21-01 compliance (mandatory controls)	IT Manager, CEO
MFA deployment for all remote access and privileged accounts	IT Manager
Annual vulnerability assessment and penetration testing	IT Manager, External vendor
SIEM implementation for threat detection (Year 2)	IT Manager, Vendor
Network segmentation (OT from IT by end Year 3)	IT Manager, Network vendor
Incident response plan with regular drills (tabletop, full-scale)	IT Manager, Consultants
Cyber insurance policy (coverage for breach response, ransom, business interruption)	Finance Manager, CEO
Phishing awareness training (annual mandatory + quarterly simulations)	IT Manager, Training vendor
Backup restoration drills (quarterly test restores to verify backups)	IT Manager, IT Specialist
Vendor security assessments (require SOC 2, security questionnaires, insurance)	IT Manager, Purchasing

Success Criteria:

- Zero successful ransomware infections (detected and blocked before encryption spreads)
- <24-hour incident response for any security breach (detect, isolate, notify stakeholders)
- TSA Security Directive compliance 100% documented and maintained

- Annual penetration and/or vulnerability testing results showing continuous improvement in reducing vulnerabilities year over year
-

Risk 2: IT Staffing Gaps and Turnover

Risk Description: Hiring and retaining qualified IT staff is challenging (small agency, market competition, limited career growth, salary constraints). Loss of Data Analyst or IT Technician after hire creates operational burden, delays projects.

Probability: 40% (Medium) - turnover within 2-3 years possible

Impact:

- **Project delays:** Data warehouse implementation stalls without Data Analyst, dashboards delayed
- **Service degradation:** IT staff departure means IT Manager returns to helpdesk firefighting vs. strategic focus
- **Knowledge loss:** Departing staff takes system knowledge, requires expensive onboarding ramp-up for replacement
- **Burnout:** Remaining IT staff overworked, negative impact on job satisfaction and retention

Mitigation Strategies:

Strategy	Responsible
Competitive compensation benchmarking (salary surveys of comparable positions, agencies)	HR Manager, IT Manager
Comprehensive benefits package (health insurance, pension, flexible schedule)	HR Manager
Clear career growth path (IT Technician → IT Specialist → Systems Administrator → IT Manager opportunity)	IT Manager, HR Manager
Professional development support (certifications, conferences, training budget)	IT Manager
Work-life balance (reasonable on-call requirements, flex schedule, avoid burnout)	IT Manager, HR Manager
Knowledge documentation and cross-training (backup for key roles)	IT Manager, IT Technician
Mentoring relationship (Planning Director or Planners to mentor Data Analyst initially)	Planning Director, Data Analyst
Regular check-ins and career discussions (quarterly with each IT staff member)	IT Manager, HR Manager
Succession planning (identify internal candidates, external candidates for backup)	IT Manager, HR Manager

Success Criteria:

- Both Data Analyst and IT Technician retained >3 years
- <20% vacancy rate in IT positions
- Staff satisfaction survey 4.0+ rating on job satisfaction and work environment

Risk 3: Budget Funding Gaps and Grant Delays

Risk Description: Technology plan assumes 80% FTA grant funding for capital expenditures. If grants delayed, denied, or reduced, projects may become unaffordable. FTA typically allocates grants October/November for next fiscal year - delays disrupt implementation timelines.

Probability: 30% (Medium) for partial shortfall, 10% for major funding gap

Impact:

- **Project delays:** Defer expensive projects (fare system, data warehouse) awaiting grant approval
- **Cost inflation:** Extended timelines increase project costs (vendor inflation, extended services)
- **Scope reduction:** Eliminate lower-priority initiatives (nice-to-have dashboards, advanced analytics)
- **Uncertainty:** Year-to-year funding uncertainty prevents multi-year vendor contracts, economies of scale

Mitigation Strategies:

Strategy	Responsible
Early FTA coordination (communicate technology priorities to ADOT/FTA early)	CEO, Finance Manager
Diversified funding strategy (5307, 5339, BIL, State,)	Finance Manager, CEO
Build contingency for local match (ensure City/County cooperation on 20% match)	CEO, Finance Manager
Apply for funding with 12-month lead time (applications December for funding spring/summer)	Finance Manager
Flexible project sequencing (reorder projects if specific grants available)	IT Manager, Steering Committee
Accept smaller incremental projects vs. all-or-nothing (spread risk)	IT Manager, Finance Manager
Maintain minimum 5% program-level contingency for unfunded shortfalls	Finance Manager
Local funding reserve (dedicated CIP funds for technology beyond FTA match)	Finance Manager, City Budget

Success Criteria:

- 90%+ of planned capital projects receive FTA grant funding (≤10% deferred due to funding gaps)

- Local match secured each fiscal year (no project delays due to match unavailability)
 - Budget variance <5% (actual spending within $\pm 5\%$ of plan)
-

Emerging Risks (Lower probability, but significant impact if occur)

Risk 4: Vendor Business Failure or Abandonment (Probability: 5%)

- Key technology vendor goes out of business
- Key contractual protection: escrow code, data ownership clauses, vendor financial stability requirements
- Mitigation: Require vendor financial statements, proof of insurance, ensure contractual protections

Risk 5: Technology Obsolescence (Probability: 20%)

- Systems deployed become outdated faster than expected (e.g., mobile app frameworks)
 - Mitigation: Cloud-first approach enables easier updates, avoid long-term vendor lock-in, build modular architecture
-

Continuous Improvement Process

Annual Strategic Review:

- Comprehensive review of all 5-year plan objectives
- Assess whether overall goals remain relevant (updates for changing environment)
- Approve any adjustments to Year 4-5 priorities

Post-Implementation Reviews:

- After each major project is completed (fare system, data warehouse, cybersecurity initiative)
 - Document lessons learned (what went well, what could improve)
 - Apply learnings to subsequent projects
 - Share with transit industry peers (APTA, SWTA forums)
-

Conclusion

Mountain Line's 5-Year Technology Strategic Plan provides a practical and forward-looking roadmap for strengthening the agency's technology foundation while supporting safe, reliable, accessible, and sustainable public transportation. It is designed to work hand in hand with Mountain Line's organization wide 5 Year Plan. By focusing on data integration, cybersecurity, infrastructure modernization, governance, and user-centered systems, the plan positions technology as a strategic enabler of better service, stronger operations, and more informed decision-making.

Successful implementation will require sustained leadership, disciplined prioritization, cross-agency collaboration, and consistent performance measurement. The plan's phased approach allows Mountain Line to balance urgency with organizational capacity, align investments with available funding, and ensure that each initiative delivers measurable value before moving to the next stage of maturity.

Over the next five years, this roadmap will help Mountain Line build a more resilient, secure, and data-driven operating environment. More importantly, it will support the agency's broader mission by improving the rider experience, strengthening internal capabilities, protecting public resources, and preparing Mountain Line to meet the evolving mobility needs of the Flagstaff community.

Appendix A: Implementation Roadmap & Phasing

Multi-Year Implementation Phasing and Dependencies

The 5-year technology plan is organized into four implementation phases balancing competing priorities, funding availability, and organizational capacity.

Phase 1: Foundation & Quick Wins (Year 1)

Objective: Establish governance structures, address critical security gaps, deploy early wins that build momentum, and lay groundwork for larger multi-year initiatives.

Phase 1 Budget Summary:

- Total Year 1 investment: **\$280-305K**
- Grant funding (80% FTA): \$224-244K
- Local match (20%): \$61K (primarily staff positions)
- Key funding sources: FTA Section 5307 (operating), Section 5339 (capital where applicable)

Phase 1 Success Metrics:

-  Technology Steering Committee meeting quarterly with 80%+ attendance
-  TSA Security Directive compliance achieved by June 2026
-  Data governance policies established and staff trained
-  Inter-facility connectivity operational with <5ms latency
-  IT Technician hired and onboarded
-  Fare system deployed
-  Zero successful ransomware attacks in Year 1

Phase 2: System Modernization & Integration (Year 2)

Objective: Deploy major system replacements (fare, fleet management), launch data warehouse with operational dashboards, strengthen cybersecurity. Assumes Data Analyst hired during this year.

Phase 2 Budget Summary:

- Total Year 2 investment: **\$780-820K**
- Grant funding (80% FTA): \$620-650K
- Local match (20%): \$160-170K
- Key funding sources: FTA Section 5307, Section 5339, BIL opportunities

Phase 2 Success Metrics:

-  Fare system Go-Live with 100% user adoption within 30 days
 -  Data warehouse producing dashboards used by 80%+ of managers
 -  SIEM implementation with <1% false positive alert rate
 -  OTP improved by 5% through data-driven service planning
 -  New vehicle camera system (REI or selected vendor) operational in 50% of fleet
-

Phase 3: Advanced Analytics & Operational Technology Security (Year 3)

Objective: Mature data analytics capabilities, advance cybersecurity to NIST CSF Level 3, modernize HR and planning systems.

Phase 3 Budget Summary:

- Total Year 3 investment: **\$445-480K**
- Grant funding (80% FTA): \$355-385K
- Local match (20%): \$90K
- Key funding sources: FTA Section 5307, Section 5310 (paratransit enhancements), discretionary grants

Phase 3 Success Metrics:

-  NIST CSF maturity Level 3 (Managed) across Govern, Identify, Protect, Detect, Respond
 -  Predictive maintenance reduces vehicle downtime by 15%
 -  HR system eliminating manual CDL/certification tracking errors
 -  Annual penetration test results showing 50% fewer vulnerabilities vs. Year 2
 -  Customer satisfaction rating improves to 4.0+ (out of 5.0)
-

Phase 4: Optimization & Continuous Improvement (Years 4-5)

Objective: Mature to NIST CSF Level 4 (Adaptive), optimize all systems based on 3+ years of operational data, plan next-generation technology investments.

Phase 4 Budget Summary (Indicative):

- Years 4-5 average annual investment: **\$300-400K**
- Grant funding (80%): \$240-320K
- Local match (20%): \$60-80K
- Budget allocation varies based on priorities (stabilization vs. innovation spending)

Phase 4 Success Metrics:

-  NIST CSF Level 4 (Adaptive) - proactive threat hunting, automated response
 -  Cost per passenger improved 15-20% through data-driven optimizations
 -  Customer satisfaction stable at 4.0+ rating
 -  Zero major technology incidents or data breaches
 -  All systems meeting or exceeding availability targets (99.9%+)
 -  Technology plan successfully transitions to next 5-year cycle
-

Risk Mitigation:

- **Budget contingency:** 15% reserve for cost overruns, unforeseen issues
- **Vendor risk:** Establish strong contracts with performance guarantees, liquidated damages for delays
- **Scope creep:** Technology Steering Committee reviews all change requests, prioritizes ruthlessly
- **Grant deadlines:** Track FTA spend-down requirements, plan procurements to align with grant periods
- **Staffing gaps:** Begin IT position recruiting in Month 2 (assuming Month 1 approval), hire contractors if permanent hires are delayed

Appendix B: Key Budget Drivers by Category

Personnel (largest recurring cost):

- Data Analyst: \$91-112K/year (salary + benefits)
- IT Technician: \$63-77K/year (salary + benefits)
- External consultants (variable): \$50-75K/year for implementation support
- **Personnel subtotal: \$204K – \$264K/year**

Major System Implementations (one-time capital):

- Fare collection system: \$410K - \$470K (hardware, software, implementation)
- Data warehouse (platform, integration, storage): \$200K - \$350K
- Network infrastructure (equipment): \$90K - \$120K
- Cybersecurity improvements (SIEM, tools, testing): \$100K - \$125K
- **Capital subtotal: \$800K – \$1.1M**

Ongoing Operating Costs (annual subscriptions/support):

- Data warehouse (platform, storage, BI tools): \$75-130K/year
- ITSM compliant ticketing system: \$5-10K/year
- Cybersecurity tools (SIEM, scanning, simulation): \$30-50K/year
- Backup and disaster recovery: \$15-25K/year
- IT support contracts (vendor maintenance): \$50-100K/year
- Professional services (support, training, optimization): \$50-75K/year
- Network operations and maintenance: \$25-35K/year
- **Operating cost subtotal: \$250-425K/year**

Appendix C: Funding Strategies

Primary Funding Sources:

1. FTA Section 5307 (Urbanized Area Formula Grants)

- **Eligibility:** Capital and operating projects for transit agencies
- **Mountain Line eligibility:** Flagstaff is designated urbanized area, Mountain Line is primary recipient
- **Funding level:** ~\$4-5M annually (based on service area population)
- **Technology eligibility:** Computer systems, software, planning, training supporting service delivery
- **Application:** Annual Unified Planning Work Program (UPWP), included in MetroPlan process
- **FTA share:** 80% (federal grant), 20% local match requirement
- **Timeline:** Grants typically awarded October/November for next fiscal year (plan ahead 18-24 months)

2. FTA Section 5339 (Bus and Bus Facilities Program)

- **Eligibility:** Capital projects for buses, facilities, equipment
- **Technology scope:** Less flexible than 5307, but includes technology directly serving transit mission (fare system, CAD/AVL, vehicle technology)
- **Application:** Annual RFP typically December-January
- **FTA share:** 80% for small and mid-size communities (80%+ of budget), 20% local match
- **Competitive process:** Agencies compete for limited funding based on applications
- **Strategy for Mountain Line:** Prioritize fare system and vehicle systems (cameras, diagnostic equipment) for 5339 eligibility; allocate data warehouse and cybersecurity to 5307

3. Bipartisan Infrastructure Law (BIL) / Infrastructure Investment and Jobs Act (IIJA)

- **Funding level:** One-time supplemental funding for transit (\$39B nationally), prioritizes EVs, equity, workforce
- **Timeline:** Most BIL funding available 2022-2026 (declining availability after 2026)
- **Technology focus:** Discretionary funding available for innovative projects (EV charging integration, real-time information, demand response, equity initiatives)
- **Application:** Typically, by December for funding announcement spring/summer
- **Strategy for Mountain Line:**
 - Years 1-2: Apply for BIL funding for paratransit/demand response technology (Spare Labs), EV fleet technology integration
 - Years 3-4: Look for remaining BIL opportunities for cybersecurity, accessible technology, community broadband/Wi-Fi at transit stops
- **BIL share:** Often 80-90% federal (varies by specific program)

4. RAISE Grants (*Rebuilding American Infrastructure with Sustainability and Equity*)

- **Eligibility:** Capital projects supporting sustainable, equitable transportation
- **Funding level:** ~\$1B annually (nationally competitive)
- **Technology scope:** Less focused on pure IT projects, but could support integrated mobility projects (MaaS, micromobility integration, real-time information networks)
- **Strategy:** Lower priority for Mountain Line given competitive nature, but could pursue for innovative community mobility projects in Years 3-5

5. State of Arizona Funding

- **Arizona Dept of Transportation (ADOT):** May have discretionary funding for transit technology (coordination, data sharing, safety)
- **Arizona Department of Health Services:** Potentially support for health equity/access technology projects
- **Arizona Commerce Authority:** Workforce development grants for training programs (IT training, technician development)
- **Strategy:** Network with ADOT and DHS on annual funding opportunities, emphasize coordination benefits

6. Local Funding (*Mountain Line Match and General Revenue*)

- **Local match requirement:** 20% for FTA grants (approximately \$550-650K over 5 years)
- **Sources:**
 - Mountain Line general operating revenue (currently sustainable, though margins tight)
 - Local grant matches from City of Flagstaff, Coconino County (both invested in transit)
 - Potential local government technology coordination funds (ADOT/DHS provide matching funds if Mountain Line coordinates)
- **Strategy:** Budget local match in annual CIP (Capital Improvement Program), avoid contingency on external grants

7. Private Grants and Philanthropic Support

- **Potential sources:**
 - Knight Foundation (invests in tech-enabled cities)
 - Google.org (supports sustainable transportation, AI for social good)
 - Smart Growth America
 - Transit-focused organizations (APTA, RTAP, Transportation Alternatives)
- **Likely technology fit:** Mobility innovation, accessibility enhancements, data sharing/open data initiatives
- **Strategy:** Lower priority due to small award sizes (\$25-100K typical), but explore for specific initiatives (e.g., accessibility advisory committee, crowdsourcing apps, open data portal)

Potential Grant Application Strategies

Year 1 - Secure Funding for Years 1-3:

Action	Funding Source	Amount	Notes
Submit FTA Section 5307 application (current year)	FTA 5307	\$500K	For implementation starting mid-2025
Apply for FTA Section 5339 - Fleet equipment	FTA 5339	\$300K	Vehicle cameras, diagnostic equipment
Apply for remaining BIL funding (last year)	BIL	\$400K	Paratransit tech, EV charging integration
Follow-up FTA Section 5307 for next cycle	FTA 5307	\$600K	For FY 2026 projects (Months 1-12)
Apply for FTA Section 5339 (next cycle)	FTA 5339	\$300K	Fare system hardware, network infrastructure
Finalize State/Local match commitments	Local/ADOT	\$150K	Coordinate with ADOT for matching support
		\$2.75-3.45M	66% FTA grants, 34% local/other

Budget Management and Tracking

Finance Manager Responsibilities:

- Track all technology project budgets (capital and operating)
- Reconcile actual spending vs. budget monthly
- Report variance to Technology Steering Committee quarterly
- Track FTA grant compliance (eligible uses, documentation, close-out procedures)
- Ensure 20% local match availability before committing to grant-funded projects

Project-Level Budgeting:

- Each major project (fare system, data warehouse, fleet management, etc.) managed as separate cost center
- Project manager accountable for staying within budget

- Change order process for scope changes (Technology Steering Committee approval required if cost >10% of original budget)
- Post-implementation review documents actual vs. planned costs, lessons learned for future projects

Contingency Management:

- **5% program-level contingency:** %5 of annual, pre-budgeted for emergencies, unforeseen costs based on other funding sources
- **15% project-level contingencies:** Included in individual RFPs/contracts (vendor responsible for over-runs within this range)
- **Risk-based approach:** Higher contingency for novel initiatives (fare system, data warehouse) vs. lower for proven solutions