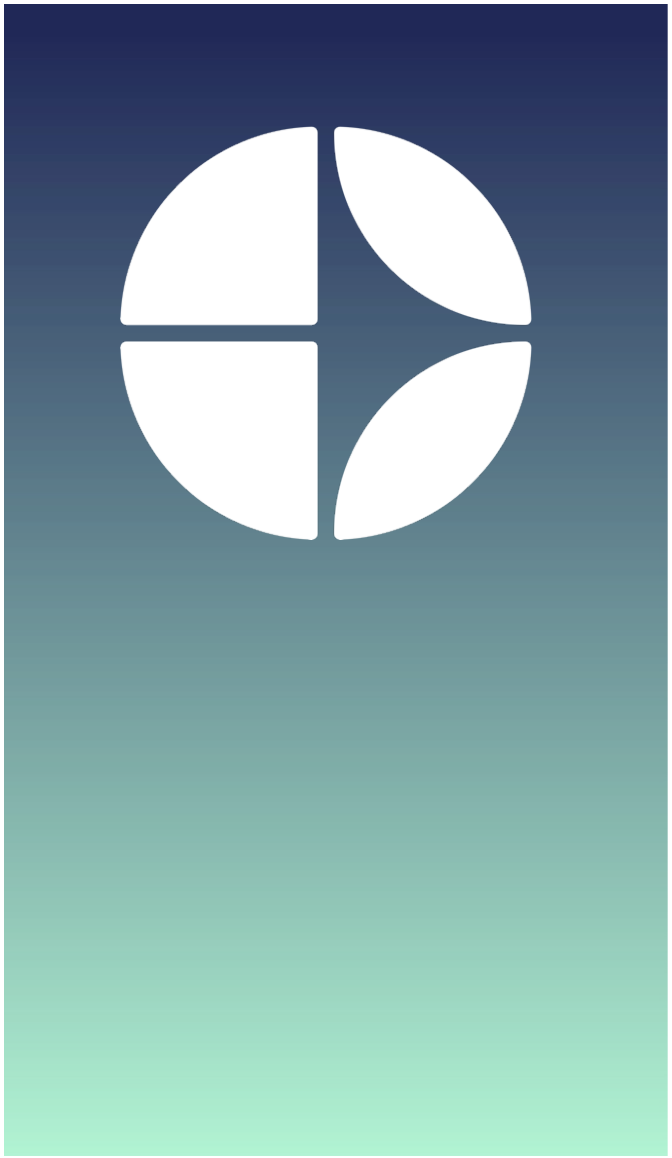

ECONOLITE
part of Umovity
Cybersecurity Compliance:
A Digital Infrastructure Imperative
17 June 2026
ITS-NY
Intelligent Transportation Society of New York



01 Transportation as Critical Digital Infrastructure

02 The Transportation Cybersecurity Challenge

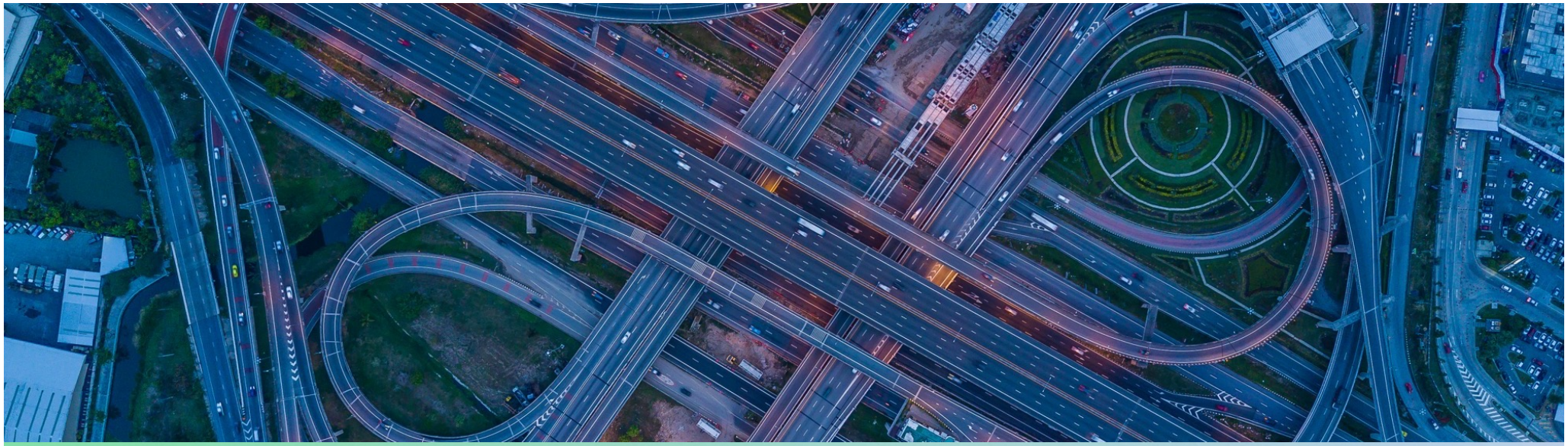
03 Understanding Today's Compliance Frameworks

04 The Real Cost of Cybersecurity Compliance

05 Lessons Learned from Industry Implementation

06 North America's Opportunity to Lead

ECONOLITE
part of Umovity



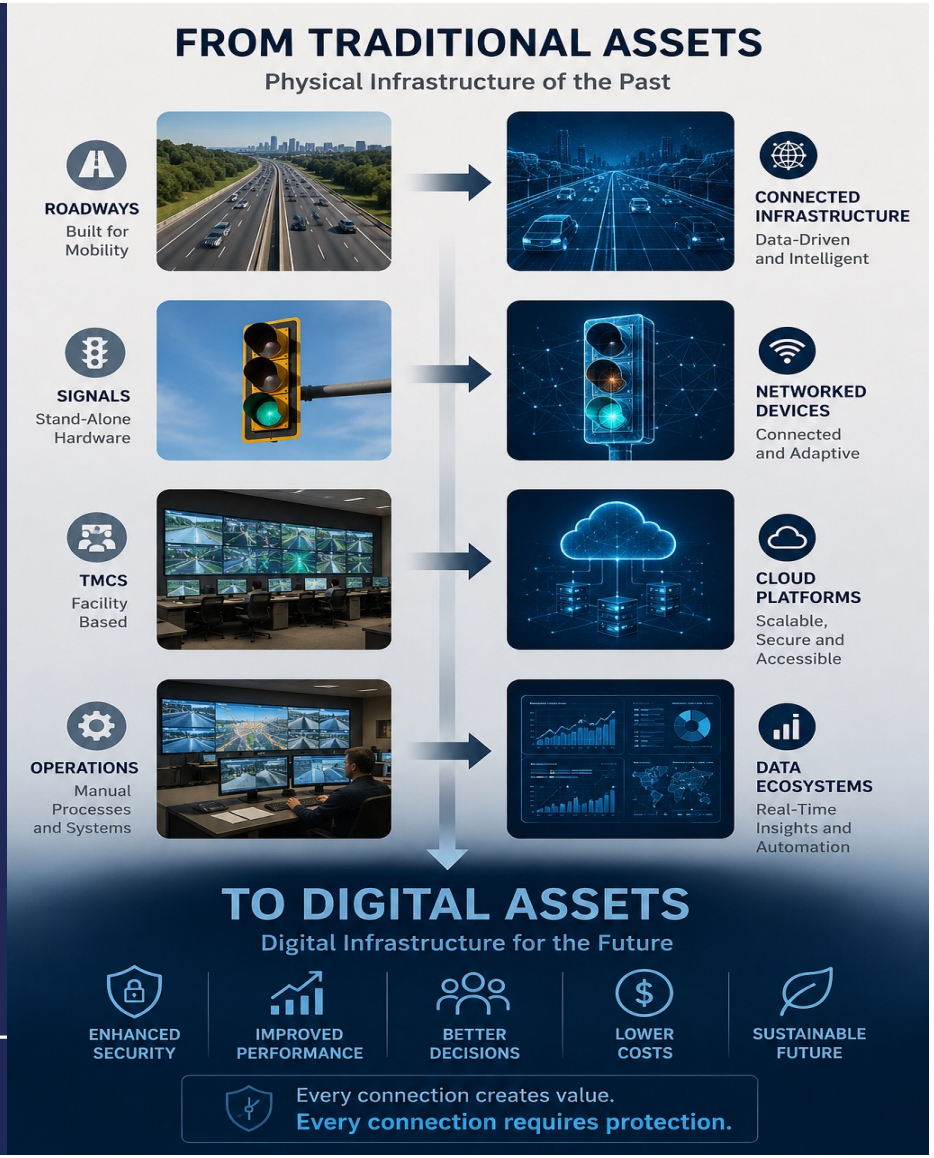
Transportation as Critical Digital Infrastructure

Why cybersecurity has become a transportation imperative

ECONOLITE
part of Umovity

Why this Matters

- Transportation assets have undergone a massive transformation.
  - Roadways become connected infrastructure
  - Signals are IOT devices
  - Traffic management centers increasingly operate cloud-based platforms.
  - Operations are becoming data eco systems to create additional data flows.
- Every connection creates value—but every connection also creates exposure.



ECONOLITE
part of Umovity

The Transportation Cybersecurity Challenge

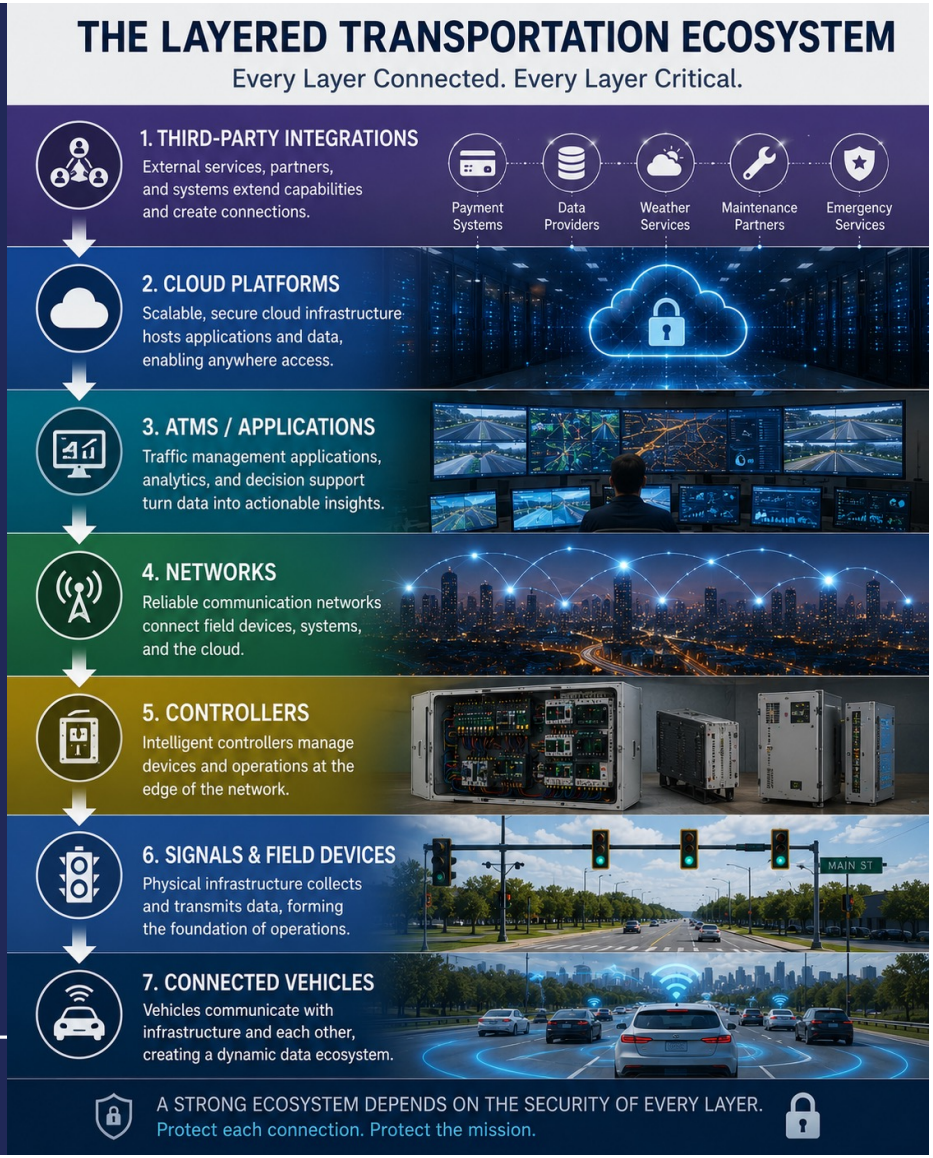
Emerging threats, risks, and operational impacts

ECONOLITE
part of Umovity

The Transportation Cybersecurity Threat Landscape

- Cybersecurity threats have evolved significantly.
- Attackers rarely target field devices directly.
- Instead they target:
  - User credentials
  - Cloud environments
  - APIs
  - Third-party vendors
  - Software supply chains

ECONOLITE
part of Umovity



Understanding Today's Compliance Frameworks

SOC 2, SOC 3, ISO 27001, TX-RAMP, FedRAMP, and GDPR

THE COMPLIANCE MAZE

Multiple Frameworks. One Goal: Trusted & Secure Transportation Systems.

Different frameworks. Shared foundation. Stronger together.

GOVERNANCE & MANAGEMENT
Establishes policies, risk management, and continuous improvement across the organization.

OPERATIONAL ASSURANCE
Independent audit of controls across five Trust Services Criteria.

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

STATE CLOUD ASSURANCE
Security framework for Texas state agencies based on NIST 800-53 controls.

FEDERAL CLOUD AUTHORIZATION
Rigorous security assessment, continuous monitoring, and ongoing authorization for federal use.

GLOBAL PRIVACY COMPLIANCE
Protects personal data and individual rights for users across the European Union and beyond.

DIFFERENT FOCUS. SHARED FOUNDATION.

These frameworks address different needs, but they rely on the same core security principles.

STRONGER TOGETHER. BUILT FOR TRUST.

Together, they provide the transparency, assurance, and trust needed for modern digital transportation.

A SECURE FOUNDATION FOR WHAT MOVES US.

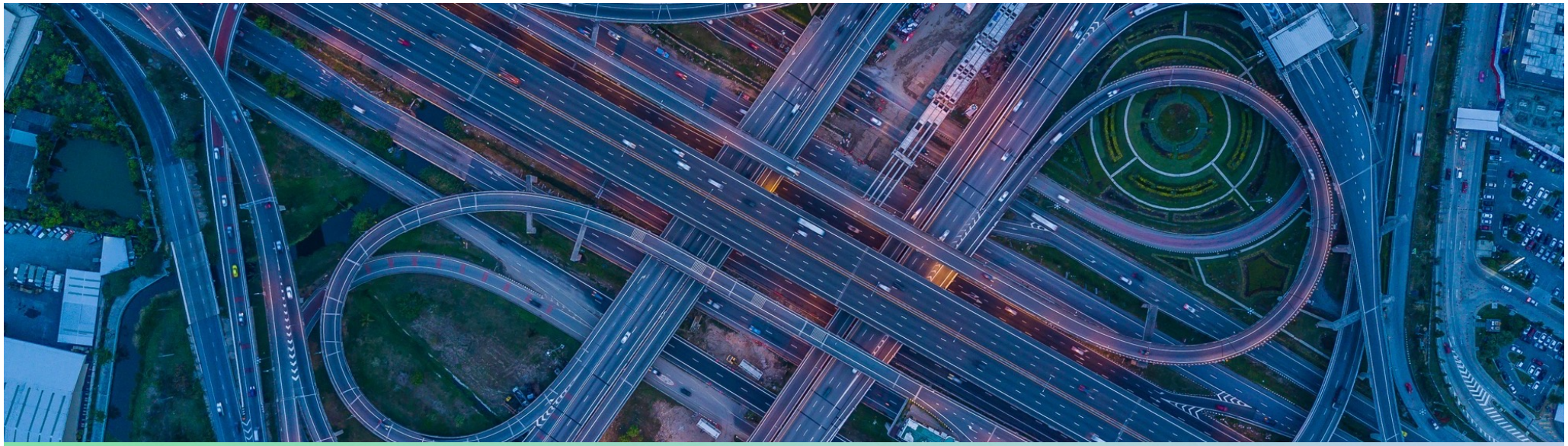
Cybersecurity compliance isn't a destination—it's a journey of continuous improvement, collaboration, and commitment to protecting the future of mobility.

Comparing the Major Frameworks

Framework	Focus	Audit Type	Geographic Scope
SOC 2	Operational Controls	Independent Audit	Global
SOC 3	Public Attestation	Independent Audit	Global
TX-RAMP	Texas Government Cloud	State Assessment	Texas
FedRAMP	Federal Government	Federal Authorization	USA
ISO 27001	Security Management System	Certification	Global
GDPR	Privacy Regulation	Regulatory Compliance	Europe

Overlap and Intersections

Control	SOC 2	ISO 27001	TX-RAMP	FedRAMP	GDPR
Access Control	✓	✓	✓	✓	
Encryption	✓	✓	✓	✓	✓
Incident Response	✓	✓	✓	✓	
Privacy Controls	✓				✓
Continuous Monitoring	✓	✓	✓	✓	



The Real Cost of Cybersecurity Compliance

Audits, continuous monitoring, governance, and organizational commitment

ECONOLITE
part of Umovity

The Hidden Cost of Compliance

- Most people focus on audit costs.
- The larger costs are:
  - Security personnel
  - Monitoring platforms
  - Penetration testing
  - Vulnerability Management
  - Documentation
  - Security Training
  - Remediation
  - Legal and Compliance Reviews

ECONOLITE
part of Umovity

Lessons Learned from Industry Implementation

Practical experience achieving and maintaining compliance

ECONOLITE
part of Umovity

What Agencies Should Ask?

- Checklist
  - SOC 2?
  - SOC 3?
  - ISO 27001?
  - TX-RAMP?
  - Vulnerability Management?
  - Incident Response Plan?
  - Annual Pen Testing?
  - Third-Party Audits?
- Who audits you?
- How often?
- How do you manage vulnerabilities?
- How do you respond to incidents?
- How do you monitor your environment?

ECONOLITE
part of Umovity

North America's Opportunity to Lead

Exporting secure transportation technology and cybersecurity best practices globally

ECONOLITE
part of Umovity

Importing Innovation to Exporting Leadership

- Checklist
  - SOC 2?
  - SOC 3?
  - ISO 27001?
  - TX-RAMP?

- Who audits you?
- How often?
- How do you manage vulnerabilities?
- How do you respond to incidents?
- How do you monitor your environment?

ECONOLITE
part of Umovity

Thank you!

econolite.com

Jon Ringler, PE
Vice President
jringler@econolite.com
678.641.9236