



Cybersecurity Compliance:

A Digital Infrastructure Imperative

17 June 2026

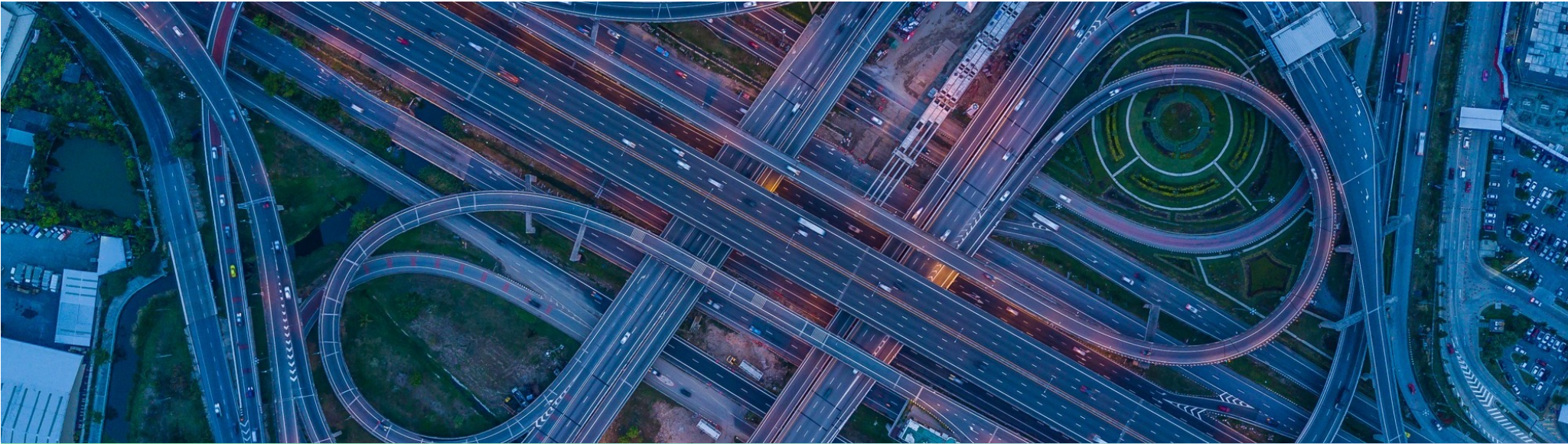


ITS-NY

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



Transportation as Critical Digital Infrastructure

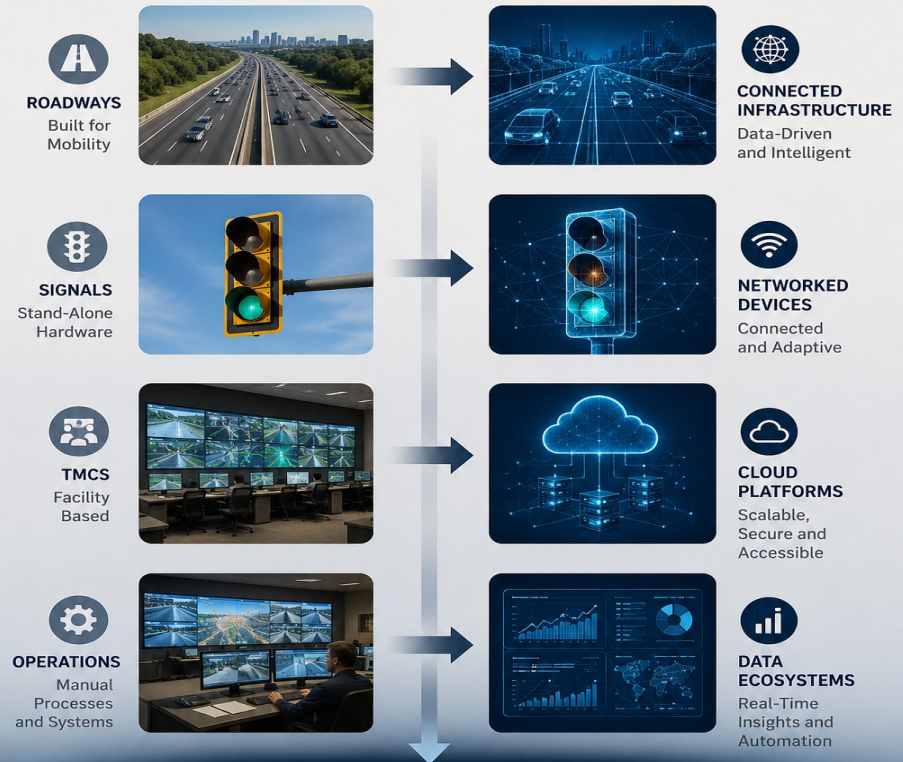
Why cybersecurity has become a transportation imperative

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.

FROM TRADITIONAL ASSETS

Physical Infrastructure of the Past



TO DIGITAL ASSETS

Digital Infrastructure for the Future



ENHANCED SECURITY



IMPROVED PERFORMANCE



BETTER DECISIONS



LOWER COSTS



SUSTAINABLE FUTURE



Every connection creates value.
Every connection requires protection.



The Transportation Cybersecurity Challenge

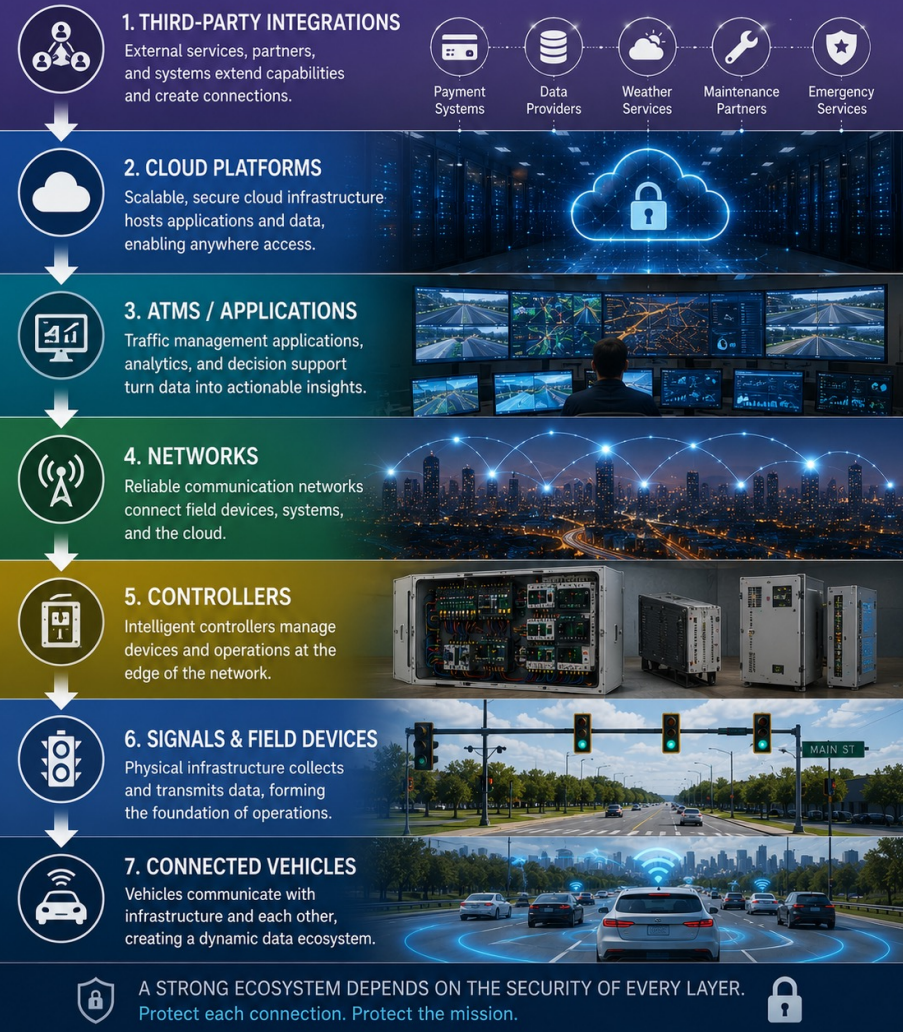
Emerging threats, risks, and operational impacts

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

THE LAYERED TRANSPORTATION ECOSYSTEM

Every Layer Connected. Every Layer Critical.





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.



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.

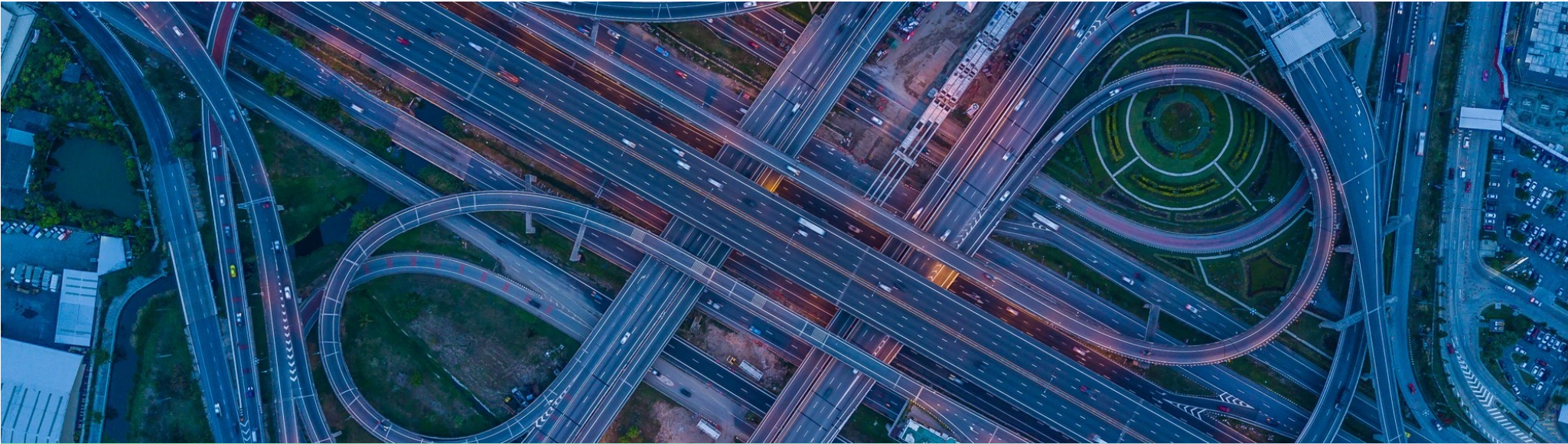
Cybersecurity compliance isn't a destination—it's a journey of continuous improvement, collaboration, and commitment to protecting the future of mobility.

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

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

THE HIDDEN COST OF COMPLIANCE

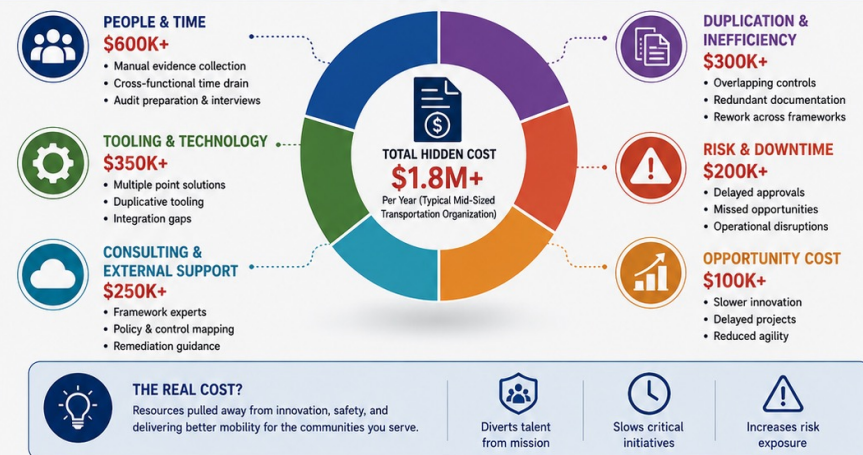
Compliance isn't just about meeting standards.
It's about the hidden costs of doing it the hard way.



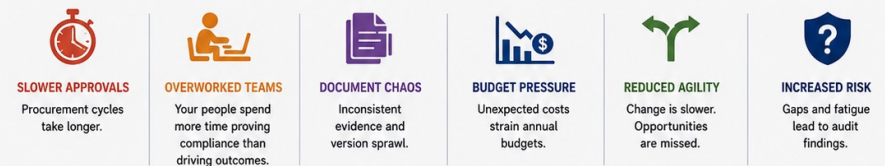
COMPLIANCE SHOULD DRIVE CONFIDENCE—NOT DRAIN RESOURCES.

Fragmented frameworks. Manual processes. Duplication. These are the hidden costs most organizations don't see coming.

WHERE THE HIDDEN COSTS ADD UP



THE CONSEQUENCES YOU FEEL



THERE'S A BETTER WAY.

Streamline compliance. Reduce hidden costs.
Free your teams to focus on what matters most.



Automate & Centralize



Standardize & Map Once



Monitor Continuously



Build Trust. Drive Impact.



Lessons Learned from Industry Implementation

Practical experience achieving and maintaining compliance

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?

WHAT AGENCIES SHOULD ASK FOR

Smart questions. Stronger security. Better outcomes.

Effective cybersecurity due diligence is about understanding maturity, not collecting sensitive information.



WHAT YOU SHOULD ASK

Focus on independent validation, processes, and continuous improvement.



Do you maintain a current SOC 2 report?



Do you provide a public SOC 3 attestation?



Are you certified to ISO 27001 or aligned with a similar framework?



Do you have a documented incident response plan?



Do you conduct regular independent penetration testing?



Do you have a vulnerability management program?



How are security findings tracked, prioritized, and remediated?



How do you monitor and respond to emerging threats?



WHAT YOU SHOULD NOT ASK

These requests can expose security risks and create unnecessary liability.



Vulnerability assessment reports



Penetration test reports



Lists of known vulnerabilities or weaknesses



Detailed security architecture or network diagrams



Why not?

These documents contain sensitive technical information that could be used by attackers to target your systems. Sharing them widely increases risk rather than improving security.



ASK INSTEAD

Instead of:

"Can we see your penetration test report?"



Ask:

"Do you conduct independent penetration testing annually?"

Instead of:

"Can we see your vulnerability report?"



Ask:

"What is your process for identifying, prioritizing, and remediating vulnerabilities?"



KEY TAKEAWAY

Evaluate cybersecurity maturity through independent certifications, governance practices, and documented processes—not by collecting sensitive technical reports that could create additional security exposure.



Independent Validation



Strong Processes



Continuous Improvement



Stronger Outcomes



Ask the right questions. Protect your systems. Build lasting trust.





North America's Opportunity to Lead

Exporting secure transportation technology and cybersecurity
best practices globally

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?

IMPORTING INNOVATION TO EXPORTING LEADERSHIP

Learn from Global Innovation.
Lead with Purpose. Build What's Next.



THE WORLD IS MOVING FORWARD—TOGETHER

Transportation challenges are global, but so are the solutions. Across the world, agencies are advancing connected systems, intelligent infrastructure, and data-driven operations. ITS-NY has the opportunity to import the best ideas—and export leadership in how we apply them.



IMPORT INNOVATION

Be curious. Be connected. Be intentional.

- Learn from leading agencies and industry pioneers worldwide.
- Adopt proven technologies and practices that accelerate our progress.
- Leverage global standards and frameworks to strengthen our systems.
- Bring innovative ideas home and adapt them to our unique communities.



EXPORT LEADERSHIP

Share our experience. Inspire others. Elevate the industry.

- Lead with the solutions we develop and the results we achieve.
- Share knowledge, lessons learned, and best practices.
- Collaborate with peers across the U.S. and around the world.
- Position New York as a global leader in safe, smart, and sustainable transportation.

A SHARED COMMITMENT

 Safety First Protect people in every decision.	 Technology Forward Embrace innovation that drives outcomes.	 Stronger Together Partnerships multiply our impact.	 Sustainable Future Build systems that last for generations.	 Global Impact Our leadership today shapes tomorrow.
---	--	--	--	--

LET'S LEARN. LET'S LEAD. LET'S SHARE.

By importing innovation and exporting leadership, we create a stronger future for all.



Learn → Apply → Lead → Inspire

Thank you!



econolite.com

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