



September/October 2026 | [www.itsinternational.com](http://www.itsinternational.com)

# International<sup>®</sup>

ADVANCED TECHNOLOGY FOR TRAFFIC MANAGEMENT AND URBAN MOBILITY



## Korea defining

ITS on the streets  
of Gangneung

### Also...

- Vamos, Barcelona!
- Quarterhill's Chuck Myers:  
'You have to be entrepreneurial'
- How AI can help disabled travellers



Dailynews

Latest news from ITS World Congress 2026 • [www.itswclive.com](http://www.itswclive.com)

**North  
America** Edition



# Security detail

Cloud-based advanced traffic management system security compliance is now a digital infrastructure imperative. Econolite's Hans M. Molin and Vincent Mayeda explain why.

**A**s roadway infrastructure adopts and deploys more connected and cloud-based systems, maintaining cybersecurity compliance with industry standards is a critically mounting requirement.

Security standards such as Systems and Organization Controls (SOC), Government Risk and Authorization Management Program (GovRAMP),<sup>1</sup> Federal Risk and Authorization Management Program (FedRAMP), and Europe's General Data Protection Regulation (GDPR) establish rigorous frameworks for protecting sensitive data, ensuring system integrity, and maintaining user privacy.<sup>2</sup>

These frameworks also provide meticulous audit benchmarks for organisational processes and policies. Compliance with these frameworks will be particularly crucial for cloud-based advanced transportation management systems (ATMS) that manage and leverage roadway data. Compliance mitigates risk and supports operational resilience. It also builds trust with public agencies and infrastructure stakeholders.

Adherence to these standards supports regulatory alignment, enhances procurement eligibility, and enables scalable innovation. Moving forward, achieving compliance with rigorous

independent cybersecurity frameworks will be imperative for the future of digital transportation infrastructure.

## Frameworks overview

Independent or third-party-certified cybersecurity audits work to verify comprehensive data security and privacy compliance. While different audits address different aspects of an organisation's responsibilities, generally, they follow industry-recognised and certified processes.

### Systems and Organization Controls cybersecurity audit

The SOC audit is governed by the American Institute of Certified Public Accountants (AICPA). It developed the SOC frameworks, which include SOC 2 Type II and SOC 3, and sets the standards for these audits to validate an organisation's cybersecurity posture and demonstrate the effectiveness of their internal controls.<sup>3</sup> The AICPA also established the 'Trust Services Criteria (TSC): Focusing on the trust principles of Data Security, Availability, Processing Integrity, Confidentiality, and Privacy'. These criteria underpin a voluntary audit provides third-party assurances about a platform and the cloud service provider's (CSP) internal controls over a period

of time. Requiring ongoing compliance validation, it also verifies the operational effectiveness of these controls.

### Risk and authorisation management programs

GovRAMP and FedRAMP are closely related cloud security frameworks.

FedRAMP, funded by the Federal Office of Management and Budget, is a US government-wide programme that standardises the security assessment, authorisation, and continuous monitoring of cloud-based products and services used by government agencies. It was created to accelerate the adoption of cloud-based computing by providing a government-wide security baseline.

GovRAMP, a non-profit, is specifically designed for state, local, tribal and educational (SLED) entities to standardise the security evaluation of CSPs. This programme serves the unique needs of state and local procurement processes, ensuring CSPs meet stringent security benchmarks.

Both GovRAMP and FedRAMP require continuous monitoring and assessment.

### General Data Protection Regulation

GDPR is a mandatory, legally enforceable regulation framework that governs the processing of personal data of European

Union (EU) residents. A GDPR audit assesses a company's lawful compliance with data protection principles, including processing, subject rights and security measures. In the case of GDPR, non-compliance carries significant penalties.<sup>4</sup>

### Compliance to industry security standards for cloud-based ATMS software

Municipalities are deploying and implementing more cloud-based solutions to manage traffic safety, roadway infrastructure, and emerging mobility applications. As a result, cybersecurity compliance with industry security standards is essential.

Auditing and evaluation frameworks like SOC 2 Type II, GovRAMP and GDPR provide structured third-party validation of security, privacy and operational controls. This helps to demonstrate that not only is the platform resilient, trustworthy and aligned with regulatory expectations but also that the organisation adheres to the highest standards for security processes and policies. This is especially important for CSPs and a cloud-based ATMS platform.

### Data security and trust

Cloud-based ATMS platforms handle growing volumes of roadway data, including traffic patterns, infrastructure telemetry and user information. SOC 2 Type II audits validate not only the existence of security controls but also their operational effectiveness over time. This instills long-term confidence in the platform's ability to protect data against breaches and unauthorised access. GDPR further reinforces this by mandating strict data handling, consent and breach notification protocols for any system processing personal data.

GovRAMP requires that cloud services meet stringent security baselines. In many cases, this is mandatory for public-sector technology procurement and deployments.

### Operational excellence and risk management

Compliance frameworks mandate best practices that directly enhance ATMS resilience. SOC 2 requires robust access controls, encrypted communications, and continuous monitoring. It verifies that only authorised users can interact with critical systems. The process audits enforce vulnerability scanning, incident response planning, and configuration management, which are vital for maintaining uptime and mitigating threats. Furthermore, ATMS platforms will require verification of controls for data minimisation and accountability mechanisms.

These controls reduce operational risk, prevent service disruptions, and enable proactive threat detection. This is a critical competency for systems that must operate reliably in real-time transportation environments.

### Smart city assurance

Compliance certification is often a prerequisite for doing business with government agencies and enterprise clients in today's procurement landscape, and this will be more of a requirement in the future.

Departments of transportation (DoTs), municipal planning organisations (MPOs), and traffic engineering agencies increasingly require SOC 2 Type II audit or GovRAMP certification as part of their vendor selection criteria. GDPR compliance is essential for any ATMS provider operating in or serving EU jurisdictions.

These certifications serve as differentiators, signalling that a vendor meets the industry's highest standards for security and privacy. They also streamline procurement by reducing the need for custom security assessments.

### Regulatory alignment and vendor trust

Cybersecurity compliance aligns cloud-based ATMS platforms with evolving regulatory requirements.

SOC 2 and ITS International North America Sept 2 provide structured documentation and audit trails. The comprehensive audits and compliance help to show that data subjects' rights are respected, and that systems are designed with privacy in mind.

Importantly, these frameworks allow cloud providers to rely on third-party assurances rather than duplicative internal-based audits, which lack transparency. Third-party audits build ATMS platform trust with customers, regulators, and integration partners.

### TSC compliance and internal process policies

Standards-based and industry-recognised cybersecurity frameworks are built around core principles designed to ensure data security, availability, processing integrity, confidentiality and privacy of cloud-based systems. These trust principles are part of the TSC and can be directly mapped to internal process policies that govern the development and operation of cloud-based ATMS (Figure 1).

The alignment between these standards and internal controls demonstrates a proactive approach to compliance and risk mitigation. It also requires a continual improvement process and re-certification programme.



Figure 1: Trust services criteria core principles.



Here are a few of the comprehensive suite of policies, including data protection, network security, and encryption, as they relate to the TSC principles.

### Security

Security is foundational to all compliance frameworks. SOC 2 and GovRAMP require strict network isolation, intrusion detection systems (IDS), and firewall configurations to prevent unauthorised access.

For example, a comprehensive network security policy is essential. It enforces process controls through segmented network zones, ACLs and firewalls that isolate production environments from external threats. This is vital for the organisation and the product.

In addition, secure remote access protocols such as VPN, SSH, and TLS 1.2 or higher are mandated, helping to ensure encrypted communication across untrusted networks.<sup>5</sup> These measures directly address specific security criteria and designated baseline controls for cloud-based services and systems.

### Availability

Data availability is critical for ATMS platforms that manage real-time traffic operations. It is imperative that processes require redundancy, disaster recovery and infrastructure monitoring to maintain system uptime.

A comprehensive data protection policy is essential. It outlines the use of multi-zone replication and encrypted storage volumes to maintain data availability. The policy must also outline the use of security information and event management (SIEM) tools to detect system failures and trigger alerts, supporting rapid response and continuity of service.

These practices align with SOC 2's availability criterion and GovRAMP's continuous monitoring requirements.

### Processing integrity

Processing integrity requires systems operate accurately and reliably. SOC 2 requires mechanisms to prevent unauthorised data manipulation and to log all system activities.

As a result, a data protection policy must mandate role-based access control and comprehensive audit logging for create, read, update and delete (CRUD) operations. Logs capture who performed the action, what was done, and the outcome. This is necessary for forensic analysis and compliance reporting.

These controls help to maintain ATMS data remains accurate and trustworthy.

### Confidentiality

Protecting sensitive data from unauthorised disclosure is especially important for using real-time crowd-sourced or floating car data (FCD). For example, there are audit benchmarks for encryption of personal data at rest and in transit. This is where an encryption policy that specifies the use of symmetric and/or asymmetric encryption standards for all data, including VPN keys, SSL certificates and internal communications, is essential.

Moreover, combined with a stringent data protection policy, the use of encryption standards reinforces data confidentiality controls by requiring trusted encrypted volumes and secure key management practices. This also includes rotation and hardware-backed storage, helping to protecting confidential traffic data and user information in accordance with industry and international standards.

### Privacy

A central tenet of GDPR, privacy is increasingly emphasised in the SOC 2 Type II evaluation. A data protection policy must include data classification protocols, encrypted messaging channels, and regulated data transfer mechanisms. Sensitive data is logically separated at the

database level, and access is restricted through token-based authentication.

These measures ensure personal data is protected and accessible. ITS International North America Sept 2026  
accountancy, privacy regulations and customer expectations.

### Optimised security posture

In the realm of smart mobility and cloud-based ATMS, cybersecurity compliance is an operational imperative that demonstrates a culture of security.

Transportation agencies, cities and MPOs demand assurances that their cloud-based platform and operational data is protected by rigorous, independently verified controls. SOC 2 Type II, GovRAMP, and GDPR security frameworks provide that assurance, validating accredited third-party auditing of security measures with a focus on sustained ongoing improvement and effectiveness over time.

SOC 2 Type II audits, for example, demonstrate that a cloud-based ATMS provider has implemented controls aligned with the TSC: security, availability, processing integrity, confidentiality, and privacy. These controls must show they are actively monitored and maintained. This level of transparency fosters trust among public-sector clients, who must demonstrate that their systems meet internal governance and external regulatory requirements. GDPR compliance further reinforces this trust by guaranteeing personal data is handled ethically and securely, with accountability and breach notification protocols.

In addition, security frameworks compliance drives a stronger security posture. Preparing for SOC 2 or GovRAMP evaluation audits requires organisations to formalise and document security practices, implement continuous monitoring, and establish incident response procedures.

Receiving a clean 'no exceptions' report for a cloud-based platform reflects the highest levels of commitment to an optimised security posture. It also confirms that policies directly address network segmentation, intrusion detection, and encrypted remote access. They also identify and enforce encryption and strict key management practices, as well as detail data classification, logging and monitoring protocols.

These controls also elevate and validate the organisation's ability to detect, respond to, and recover from threats. Real-time monitoring tools, centralised logging, and role-based access controls help identify and address anomalies quickly. The result is a resilient cloud-based ATMS platform capable of supporting critical infrastructure in dynamic, even unpredictable, ecosystems.

By aligning internal policies with industry standards, cloud-based ATMS platforms and their providers demonstrate technical competence and strategic foresight. This also supports system scalability and flexibility to support emerging technologies and applications.

As cloud-based ATMS become central to smart city mobility infrastructure, aligning with cybersecurity frameworks like SOC 2 Type II, GovRAMP, and GDPR is vital. These industry security standards not only validate the robust security controls of CSPs but also demonstrate that the cloud architecture is designed for resilience, scalability and integrity.

Leveraging and incorporating multi-zone replication, encrypted volumes and automated monitoring tools support high availability and rapid incident response. These few architectural examples reflect a deep commitment to safeguarding sensitive traffic and infrastructure data while supporting operational continuity.

To maintain compliance and maximise the benefits of these cybersecurity frameworks, a continually monitored, structured approach is needed for cloud-based ATMS development.

A few vital areas should include:

- **Planning** – gap analysis against framework requirements. Identify areas where internal policies and technical

controls need enhancement, particularly around data classification, access management and encryption.

- **Conducting audits** – engage with AICPA-certified third-party auditors to perform SOC 2 Type II assessments. Audit readiness should include comprehensive documentation, centralised logging and evidence of control effectiveness over time.
- **Ongoing compliance** – cybersecurity is a continuous process. Implement automated monitoring, regular vulnerability scans, and incident response drills. Update policies to reflect evolving threats and regulatory changes. Maintain audit trails and conduct annual reviews of firewall rules, access controls, and encryption standards. Ensure scheduled audits, certifications and attestations are fulfilled.<sup>6</sup>

By embedding these cybersecurity practices into the foundation of a cloud-based ATMS, CSPs not only meet compliance requirements but also optimise their security posture. This is fundamental in building stakeholder trust and better positioning the system for scalable growth.

In the context of smart city integration, where data flows across public and private networks, this cybersecurity diligence help

to ensure digital mobility infrastructure maintains the highest levels of security and interoperability. **ITS**

## References

1. StateRAMP (dba GovRAMP), a 501(c)(6) nonprofit, is a membership organisation composed of service providers offering IaaS, PaaS, and/or SaaS solutions, third party assessment organisations, and government officials. Its members lead, manage, and work in various disciplines across the United States and are all committed to making the digital landscape a safer, more secure place. <https://govramp.org>
2. GovRAMP and FedRAMP derive from NIST SP 800-53 requirements; GDPR mandates technical-organisational measures for personal data. <https://www.compliancepoint.com/cyber-security/comparing-fedramp-and-govramp/>; <https://www.gdpr-advisor.com/gdprcloudsecurity/>; <https://www.databank.com/resources/blogs/understanding-gdpr-cloud-compliance-a-guide-for-businesses/>
3. The Importance of SOC 2 Type II Compliance for Cloud Service Providers, Gateway Group April 1, 2025. <https://gatewaygroup.com/the-importance-of-soc-2-type-ii-compliance-for-cloud-service-providers/>
4. The GDPR legal requirements and penalties; GDPR Regulation (EU) 2016/679 (General Data Protection Regulation). <https://gdpr.eu/tag/gdpr/>
5. SOC 2 Requirements: Essential Guidelines for Compliance," Gowsika, Sprinto, Nov. 7, 2024 (VPN, TLS 1.2+).
6. GovRAMP requires documented continuous monitoring and incident response. StateRAMP Continuous Monitoring and Improvement Guide v1.7, September 2024. <https://govramp.org/wp-content/uploads/2022/11/StateRAMP-Continuous-Monitoring-Guide-1.7.pdf>



## The Prime Mover in Intelligent Traffic Solutions

Q-Free delivers open, secure, and scalable systems that advance tolling, transform traffic management, and pioneer new road user charging models. Trusted across Europe, Asia, Australia, and the Americas to modernize mobility and simplify every journey.

**Modern mobility starts here.**



[www.q-free.com](http://www.q-free.com)