APTA STANDARDS PROGRAM
RECOMMENDED PRACTICE

APTA SS-ECS-RP-006-25
First Published: May 27, 2025

Enterprise Cyber Security Working Group

Managing Cloud Vendor Risk

Abstract: This recommended practice establishes considerations for public transit chief executive officers, chief information officers and procurement executives interested in managing cloud vendor risk strategies for their organizations. It details practices and standards that address managing cloud vendor risks.

Keywords: advanced persistent attacks, cyber, cybersecurity assessments, cyber assets, disaster recovery, enterprise cybersecurity, fallback, information security (INFOSEC), information and communication technology (ICT), information security, intrusion detection, redundancy, resiliency, secure cloud, software as a service (SaaS), system penetration

Summary: Managing cloud vendor risks is a growing concern for public transit managers as control and management systems increasingly depend on various cloud services. These systems are vulnerable to increasingly sophisticated direct and indirect cyberattacks. The typical transit-based information technology infrastructure comprises a complex and interconnected series of components, subcomponents and services. This complexity increases the exposure of these systems to threats. Given these increasing risks, the transit industry and its technology managers must take proper steps to ensure the security of their cloud services. The development of a program should include a vulnerability assessment and mitigation, system resiliency and redundancy, and disaster recovery.

Foreword

The American Public Transportation Association is a standards development organization in North America. The process of developing standards is managed by the APTA Standards Program's Standards Development Oversight Council (SDOC). These activities are carried out through several standards policy and planning committees that have been established to address specific transportation modes, safety and security requirements, interoperability, and other topics.

APTA used a consensus-based process to develop this document and its continued maintenance, which is detailed in the manual for the APTA Standards Program. This document was drafted in accordance with the approval criteria and editorial policy as described. Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

This document was prepared by the Enterprise Cyber Security Working Group as directed by the Security and Emergency Management Standards Policy and Planning Committee.

This document represents a common viewpoint of those parties concerned with its provisions, namely transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any recommended practices or guidelines contained herein is voluntary. APTA standards are mandatory to the extent incorporated by an applicable statute or regulation. In some cases, federal and/or state regulations govern portions of a transit system's operations. In cases where there is a conflict or contradiction between an applicable law or regulation and this document, consult with a legal adviser to determine which document takes precedence.

This is a new document.

Table of Contents

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Enterprise Cyber Security Working Group**, which provided the primary effort in the drafting of this document.

At the time this standard was completed, the working group included the following members:

Dr. Julius Smith, Chair, *Dallas Area Rapid Transit*
Ahmed Idrees, Vice Chair, *Sound Transit*

Lee Allen, *Transportation Security Administration*
Peter Anderson, *GCRTA*
Muneer Baig, *SYSUSA*
Michael Bosche Sr., *OCTA*
Alesia Cain, *Clever Devices Ltd.*
Timothy Coogan, *Regional Transportation District*
Rachel Deen, *Transit Safety & Security Solutions*
Terry Follmer, *CapMetro*
Donald Luey, *Foothill Transit*
Clare Mueting, *TSA*
Sean Ryan, *MTA Metro-North Railroad*
John Sherman, *Hampton Roads Transit*
Dan Sullivan, *Regional Transportation District*
Anthony Tisdale, *FTA*
William Tsuei, *Access Services*
Jeff Van Wingerden, *Sound Transit*
Leigh Weber, *Cybersecurity Analysis Ltd.*

Project team

Polly Hanson, *American Public Transportation Association*
Michael Echols, *Max Cybersecurity LLC, ECSWG facilitator*
Brian Heanue, *American Public Transportation Association*

Introduction

This introduction is not part of APTA SS-ECS-RP-006-25, "Managing Cloud Vendor Risk."

This document is intended primarily for cybersecurity, information security and risk management practitioners or other individuals with information security responsibilities at small to medium-sized transit agencies. It also intends to recommend considerations when developing an access authentication management plan.

Scope and purpose

This document provides information on and considerations for managing cloud vendor risks within a public transit enterprise. This document is not a substitute for a cloud vendor risk management program. Nothing in this document should be taken to contradict standards and guidelines made mandatory by local, state or federal governments.

Managing Cloud Vendor Risk

1. Why cloud services will continue to grow

Companies are embracing cloud services for the following reasons: cost reduction, business agility with instant scalability, access to innovation in real time, and the ability to support business needs and requirements faster. Depending on the cloud model chosen, most of the infrastructure and the IT "plumbing" responsibilities (hardware/software upgrades, software patching, troubleshooting, etc.) can be offloaded to the cloud providers, freeing up an agency's valuable IT staff to perform more value-added services.

> **NOTE:** Cloud systems may not be desirable to every order; they could be too old or too expensive to move to the cloud before upgrading, may not be certified to interface with other systems in the cloud, or may not be worth the expense, especially for smaller, less infrastructure-based systems, or systems that will be phased out in a few years. This could be determined case-by-case, even if the agency decides on a "cloud-first" strategy.

2. Types of cloud services and shared responsibilities

The traditional IT model has all equipment, software and data in-house on property owned by the agency. This traditional on-premises (on-prem) model has advantages and disadvantages over the three cloud service models listed below. As enterprises embrace the cloud, it is crucial that everyone involved in the cloud journey fully understand what their cloud service providers (CSPs) are responsible for and what still falls to them. This is not a new issue, but it is worth discussing again since there is so much confusion and misinterpretation of the shared responsibility models. It is critical to understand the differences between software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS):

- **SaaS:** SaaS providers, such as customer relationship management solution provider Salesforce.com and time-and-expense reporting solution provider Concur®, deliver an entire application on demand that the SaaS provider fully manages. Customers only tweak configurations and manage user access and administration to the applications. SaaS solutions should be given strong consideration for applications that are not an enterprise's core competency.
- **PaaS:** PaaS targets developers in an attempt to abstract away not only the physical infrastructure but also the various stack components, such as application servers (e.g., Apache Tomcat®), database servers (e.g., SQL Server™, MySQL™ or Oracle®), caching servers (e.g., Redis, Memcached or Varnish), and so forth.
- **IaaS:** The CSP's responsibility is to ensure that their physical data centers and infrastructure are secure, compliant, highly available and reliable. The customer's responsibility is managing the application stack, the actual applications built on top of the IaaS layer, and all the user access and administration to the cloud and the applications.

Shared responsibility models between CSPs and customers have existed for several years but are still grossly misunderstood in some organizations. Lack of clarity about who owns what responsibility can lead to reduced time to market, poor decision-making, increased complexity and suboptimal cloud experience. Enterprises must get out in front of this issue and educate themselves about the different cloud service models and the shared responsibility for each.

After an agency selects the type of cloud service structure that is best to support its goals, it will need to begin thinking about the life cycle approach from the cradle to the grave that must be put in place to evaluate and monitor this risk throughout the contract's life, starting with the vendor selection process.

3. Evaluating vendor risk profiles

An IT security professional must carefully evaluate the confidentiality, integrity and availability (CIA) of the cloud services being procured before an agency makes any contractual commitments. The level of effort an agency will want to commit to this evaluation will depend on the CIA and the criticality of the systems and services provided. Some systems are real-time mission-critical (e.g., dispatch systems), where availability is paramount. In contrast, other methods are more static but require a higher level of confidentiality (e.g., human resources and payroll systems). Understanding the required critical recovery period and impact should the cloud service be unavailable for an extended time will play into the level of rigor an agency should put into the vendor evaluations and RFP process.

Agencies should follow their standard procurement policies and practices.

3.1 Pre-contract actions

During the pre-contract engagement, the agency should create a consistent, reliable process for vetting new vendors and create a policy for third-party risk management.

1. Determine vendor criticality and confidentiality risk levels based on internal inherent risk questionnaires.
2. Screen for potential overlap with previously established vendors.
3. Create relevant vendor risk assessment question sets for various risk levels.
4. Evaluate vendor responses to the questionnaire and assign risk-based parameters consistent with agency policy.

Agencies will want to leverage the following additional considerations in the evaluation of each cloud vendor:

- How long have they been providing cloud services, and how are their customer references?
- Do they have a recent Service Organization Control (SOC 2) report? If yes, the agency will want to review this critical IT document. If no, consider requiring that they obtain an SOC 2 within a stated period and perform this SOC 2 review annually.
- Have each vendor complete an IT Risk Questionnaire.
- Consider using this Vendor Strategic Alliance questionnaire developed from best practices: https://www.vendorsecurityalliance.org/downloadQuestionaire.
- The agency's IT security personnel should evaluate each vendor.

3.2 Post-contract activities

1. Establish a regular cadence to reevaluate vendors and detect potential risks.
2. Establish processes for issue management, remediation tracking and reporting.
3. Manage vendor performance using SLA metrics.

3.3 Other considerations

Other essential items to consider both before and after signing a contract include the following:

- cybersecurity ratings
- financial ratings
- organization of information security

- secure baseline standards
- physical and environmental security
- access control
- identification and authentication
- system security
- data isolation and segmentation
- API integration
- auditing and monitoring
- network security
- data protection, sanitization, and destruction
- incident response and notification
- business continuity management and disaster recovery

The results of these exercises should be reviewed and discussed as part of the vendor selection process.

3.4 Roles and responsibilities

Once a contract is signed, the agency will need to make sure the following roles and responsibilities are defined:

- provider
- business owner
- application owner
- service manager

4. Conclusion

Cloud computing offers potential benefits, including cost savings and improved business outcomes for organizations. However, there are a variety of information security risks that need to be carefully considered. Risks will vary depending on the sensitivity of the data to be stored or processed, as well as how the chosen cloud vendor (also referred to as a cloud service provider) has implemented its specific cloud services. These recommendations are intended to provoke discussion and help transit agencies identify and manage relevant information security risks associated with the evolving field of cloud computing.

Abbreviations and acronyms

API	application programming interface
CEO	chief executive officer
CIA	confidentiality, integrity and availability
CIO	chief information officer
CSP	cloud service provider
IaaS	infrastructure as a service
ICT	information and communication technology
INFOSEC	information security
IT	information technology
PaaS	platform as a service
RFP	request for proposal
SaaS	software as a service
SLA	service level agreement
SOC 2	System and Organization Controls

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	Oct. 4, 2024	March 3, 2025	March 27, 2025	Apr. 24, 2025	May 27, 2025