

Information Security & Technology:

Strengthen governance to protect data and investments

Why this audit is important

Metro uses information technology (IT) to collect, process, and maintain data to support operations and decision-making. IT can make Metro services more efficient and convenient to customers, but can also pose risks to information security. Information security protects information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

The audit objective was to determine if Metro’s governance structure was effective for managing information security risks by examining three areas: surveillance camera usage, payment card data protection, and cloud computing applications.

Effective governance ensures risks and resources are managed efficiently. Authority, processes and planning, and oversight are categories of effective governance.

Surveillance camera



Source: Metro Auditor’s Office photo of surveillance camera at Metro Regional Center.

What we found

Stronger governance would help Metro better manage information technology (IT) investments and information security risks. Some governance best practices were in place. However, they were not designed or carried out to effectively manage IT resources. Metro also had some practices in place to manage information security risks, but there were deficiencies that weakened the agency’s ability to protect the availability, confidentiality, and integrity of data in each of the areas we reviewed. We found:

- Metro lacked governance for surveillance camera usage.
- Governance was ineffective to achieve Metro’s goal of being compliant with Payment Card Industry (PCI) Standards.
- Governance of cloud computing would benefit from more thorough contract language and adherence to Metro’s policy.

Metro had some governance best practices partially in place to manage IT investments and information security risks

Area	Governance best practices in place		
	Authority	Processes and planning	Oversight
IT investments			
Surveillance cameras			
Payment security			
Cloud computing			

= Fully in place = Partly in place = Not in place

Source: Metro Auditor’s Office analysis of documentation and interviews related to each area.

What we recommend

We recommended Metro improve IT governance by developing a strategic plan and establishing a governance structure to oversee its implementation. We also made several recommendations to improve information security governance. Metro should develop policies and procedures for surveillance cameras, take actions to comply with PCI standards, and include more detailed language in cloud computing contracts. Metro should also publish a list of cloud storage providers and develop a long-term plan for cloud technology.