Information Security and Technology:

Strengthen governance to protect data and investments

March 2019
A Report by the Office of the Auditor

Brian Evans
Metro Auditor

Simone Rede
Senior Management Auditor

Zane Potter
Senior Management Auditor

Metro Accountability Hotline

The Metro Accountability Hotline gives employees and citizens an avenue to report misconduct, waste or misuse of resources in any Metro or Metro Exposition Recreation Commission (MERC) facility or department.

The Hotline is administered by the Metro Auditor's Office. All reports are taken seriously and responded to in a timely manner. The auditor contracts with a hotline vendor, EthicsPoint, to provide and maintain the reporting system. Your report will serve the public interest and assist Metro in meeting high standards of public accountability.

To make a report, choose either of the following methods:

Dial 888-299-5460 (toll free in the U.S. and Canada)
File an online report at www.metroaccountability.org

Brian Evans
Metro Auditor
600 NE Grand Ave
Portland, OR 97232-2736
TEL 503 797 1892, FAX 503 797 1831

MEMORANDUM

March 13, 2019

To: Lynn Peterson, Council President
Shirley Craddick, Councilor, District 1
Christine Lewis, Councilor, District 2
Craig Dirksen, Councilor, District 3
Juan Carlos Gonzalez, Councilor, District 4
Sam Chase, Councilor, District 5
Bob Stacey, Councilor, District 6

From: Brian Evans, Metro Auditor BE

Re: Audit of Information Security and Technology

This report covers our audit of information security and technology. 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. The purpose of this audit was to determine if Metro's governance structure was effective for managing information security risks by examining three areas: surveillance cameras usage, payment card data protection, and cloud computing applications. The audit was included in the FY2017-18 Audit Schedule.

We found that stronger governance was needed to manage IT investments and information security risks. Governance refers to the structures, systems, and practices an organization has in place to determine its strategic direction, oversee implementation of its work, and measure and report on performance. Effective governance ensures risks and resources are managed efficiently.

Some governance best practices were in place. However, they were not designed or carried out to effectively manage IT resources. Metro needed more strategic direction and oversight to govern surveillance camera usage. Despite having some aspects of best practices in place, efforts to address the risk of noncompliance with Payment Card Industry requirements have not been successful. Overall, we found Metro could improve its governance of cloud computing contracts through improved contract language. We also found that Metro needed to follow its information security policy and develop a long-term plan for cloud computing technology.

We have discussed our findings and recommendations with Andrew Scott, Deputy Chief Operating Officer and Rachel Coe, Director of Information Services. A formal follow-up to this audit will be scheduled within five years. I would like to acknowledge and thank all employees who assisted us in completing this audit.

Summary

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 from unauthorized access, use, disclosure, modification, or destruction.

We found that stronger governance was needed to manage IT investments and information security risks. Effective governance ensures risks and resources are managed efficiently. Elements of effective governance can be organized into three interrelated categories:

- **Authority** includes the establishment of policies and committees, as well as management of contracts and agreements.
- **Processes and planning** includes strategic plans and operating procedures.
- **Oversight** includes performance measurement and reporting.

Management of Metro's IT environment is dispersed between Information Services (IS) and other departments across Metro. IS generally supports application development and maintenance. Some applications are primarily managed by other departments.

Our review of Metro's management of IT investments found some governance best practices were in place. However, the elements Metro had were not designed or carried out to effectively manage IT resources. This reduced Metro's ability to identify IT projects that would have the biggest impact on agency goals. Shared responsibility for managing IT gave IS less authority. This made it more important for interdepartmental collaboration to get input on IT purchases.

Metro also followed some best practices to manage information security risks. Our review of surveillance camera usage, payment card data protections, and cloud computing showed Metro had some best practices in place. However, there were deficiencies that weakened the agency's ability to protect the availability, confidentiality, and integrity of data.

Metro needed more strategic direction and oversight to govern surveillance camera usage. Despite having some aspects of best practices, efforts to address the risk of noncompliance with Payment Card Industry (PCI) Standards have not been successful. We found Metro could improve its governance of cloud computing through improved contract language and implementation of its information security policy.

We recommended Metro improve IT governance by developing a strategic plan and establishing a governance structure to oversee its implementation. We also made recommendation to improve information security governance.

Background

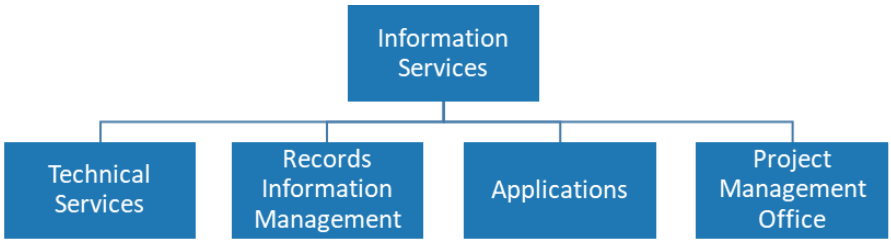
Metro uses information technology (IT) to collect, process, and maintain data to support operations and decision-making. IT refers to assets such as hardware, software, and networks. It includes the people that work with these technologies and the information that is stored, processed or produced by those systems. Technology has become increasingly critical to business and government organizations due to growing expectations from the public. IT has become a part of everyday life as society has shifted to a knowledge-based economy.

The use of IT can make Metro services more efficient and convenient to its 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. Metro departments and authorized users must protect information kept by Metro that relates to its finances and personnel, as well as information provided by Metro customers to access services. Any data that could potentially identify a specific individual, including information associated with a person who has a credit or debit card, are considered confidential. Metro is also required to manage public records in compliance with applicable laws and regulations.

Management of Metro's IT environment is dispersed between Information Services (IS) and other departments across Metro. IS generally supports application development and maintenance. Some applications are primarily managed by other departments.

IS consists of four units: Technical Services, Records Information Management (RIM) program, Applications, and the Project Management Office (PMO). Technical Services is responsible for all systems infrastructure, operations and Help Desk services, including all hardware and software to maintain Metro's network. RIM provides training, guidance, and consultation to Metro departments for managing public records. Applications is responsible for managing agency-wide applications.

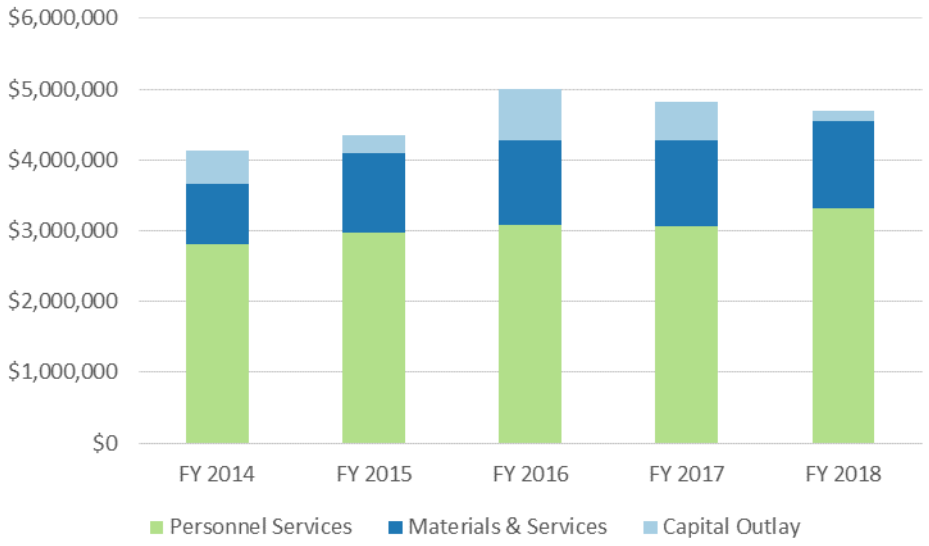
Exhibit 1 Information Services consists of four units



Source: Information Services FY 2017-18 organizational chart.

Expenditures for IS increased by about $560,000 in the last five years. Spending on Personnel Services, and Materials and Services increased during that time, while spending for Capital Outlay decreased. IS' Personnel Services budget included 30.5 FTE in FY 2017-18, an increase of 3 FTE compared to five years ago.

Exhibit 2 Expenditures for Information Services increased by 14% from FY 2013-14 to FY 2017-18



Source: Metro Auditor's Office analysis of PeopleSoft data (adjusted for inflation).

The Metro Auditor's Office has seen weaknesses in management of Metro's IT assets and risks over nearly 20 years. In 1999, we identified several areas for improvement, such as developing a comprehensive IT risk management strategy. In 2009, we found Metro was missing some key organizational elements of successful IT management. The IS department's strategic plan was out of date and had not been fully implemented. Metro also lacked an IT governance body that could prioritize projects and set standards for the agency. We recommended that Metro define the IT process, organization, and relationships. We also recommended creating a strategic plan to gradually improve IT management.

A 2013 follow-up audit found progress was made on recommendations from the 2009 audit. Metro created the IS Project Management Office (PMO) to help plan and prioritize IT projects. The IS department drafted a five-year strategic plan, which provided a description of the values, mission, and goals for the department. The plan also included a detailed list of work activities to implement the plan. The department also used Memorandums of Understanding (MOUs) to outline service level agreements between IS and the departments it served. The agreements described the purpose, background, and goals, as well as time tables and services that were not covered by the agreement. They also described how resources would be allocated and included language to resolve disputes.

However, a recent assessment showed more room for improvement. In 2017, Metro hired a consultant to review critical areas of IT and support for IS and evaluate them against best practices. The assessment found that IS was struggling to provide high-quality service to other departments. It faced obstacles to bringing IT projects to completion and struggled to keep up

with agency demand. Consultants recommended that IS review all outstanding work identified across the agency. This review was expected to be the basis for the IS department's strategic plan. Metro's FY 2018-19 budget included $150,000 for the completion of the strategic plan.

While the strategic plan may help set IT priorities for Metro, its success will likely depend on the governance structure to implement it. Effective IT governance is important not only for the IS department, but the agency as a whole. We examined three areas of IT to see whether current governance structures were effective for managing information security risks.

Surveillance cameras

Metro used surveillance cameras for both security and operations of facilities. For example, Metro's solid waste transfer stations mostly used the cameras to monitor customer service, safety, contract compliance, and to automate some business activities. At other Metro facilities, surveillance cameras were primarily used for security. For example, both Portland'5 Centers for the Arts (P'5) and the Metro Regional Center used the cameras to monitor activities outside of the facilities for safety.

In 2016, Metro contracted with a vendor to design and install security improvements at Metro facilities which included surveillance cameras. The aim of the project was to modernize and add surveillance cameras. As of September 2018, the contract had a maximum value of $2 million. About $1.3 million in payments was reported to have been spent at that time.

Payment security

Maintaining payment security is required for all entities that store, process or transmit cardholder data. The Payment Card Industry (PCI) Security Standards Council provides guidance for maintaining payment security. The breach or theft of cardholder data can cause customers to lose trust in Metro and subject them to financial loss. Metro and its customers may also pay more for transactions due to fines for noncompliance.

PCI Standards apply to entities that accept or process payment cards. They consist of several requirements. Organizations are either fully compliant or not compliant with all of the requirements. Efforts to address the risk of noncompliance with PCI Standards at Metro began in 2012.

Cloud computing

Cloud computing is the storing and accessing of data and programs over the Internet. Metro uses external service providers for some cloud computing instead of storing data on its own servers or databases. Cloud technology presents opportunities as well as risks. For example, cloud computing can reduce the amount of resources an organization puts towards IT infrastructure and maintenance, but it can also present security concerns for data that is not directly controlled by Metro. When using cloud computing vendors, governments need to protect sensitive data, maintain access to it, and ensure compliance with public records laws.

Results

We found that stronger governance was needed to manage IT investments and information security risks. Governance refers to the structures, systems, and practices an organization has in place to determine its strategic direction, oversee implementation of its work, and measure and report on performance. Effective governance ensures risks and resources are managed efficiently.

Our review of surveillance camera usage, payment card data protections, and cloud computing showed Metro had some practices partially in place to manage information security risks. However, there were deficiencies that weakened the agency's ability to protect the availability, confidentiality, and integrity of data in each of these areas. We found:

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

Exhibit 3 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* ◑ = *Partially in place* ○ = *Not in place*

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

Stronger governance was needed to manage information technology and security risks

Stronger governance would help Metro better manage information technology investments and information security risks. Elements of effective governance can be organized into three interrelated categories:

- **Authority** includes the establishment of policies and committees, as well as management of contracts and agreements.
- **Processes and planning** includes strategic plans and operating procedures.
- **Oversight** includes performance measurement and reporting.

Our review of Metro's management of IT investments found some

governance best practices were in place. In 2012, Metro created a committee to review and approve certain IT projects. It included directors from several Metro departments. We were told the committee used a formal process for evaluating and planning projects. The Information Services (IS) department documented its five-year mission-critical efforts. The document identified goals to ensure Metro was investing in and maximizing the use of IT. Metro's organizational structure assigned responsibility for managing IT to IS as well as other Metro departments. This set an expectation for departments to work together to procure and manage IT resources.

However, the elements of governance Metro had in place were not designed or carried out to effectively manage IT resources. In 2015, the prioritization committee was disbanded. We were told the projects it prioritized were not initiated. This reduced Metro's ability to identify IT projects that would have the biggest impact on agency goals.

The mission-critical efforts IS documented were not prioritized. This made them more difficult to deliver. The department engaged in additional strategic planning activities during our audit. This made it hard to tell which goals the department was pursuing to achieve its mission. Shared responsibility for managing IT gave IS less authority. This made it more important for interdepartmental collaboration to get input on IT purchases and reach agreement about who would be responsible for ongoing support of IT systems. For these reasons, governance of IT resources was ineffective.

Metro also followed some best practices to manage information security risks. However, there were deficiencies that weakened Metro's to ability protect information in the three areas we reviewed in this audit.

We found that Metro followed some aspects of best practices for governing security camera usage, such as the development of policies for the retention of surveillance recordings. Retention policies help Metro comply with public records laws and ensure public access to records. The policies document how long each type of recording should be maintained.

Metro followed some aspects of best practices to address the risk of noncompliance with PCI Standards. These include having structures in place to more effectively govern. Policies are one way to provide direction for an organization's activities. We found Metro's information security policy provided direction for protecting cardholder data. It defined cardholder data as confidential and assigned responsibility for securing cardholder data and systems to departments and users. The policy also referenced PCI Standards. These elements helped set clear expectations for protecting cardholder data at Metro.

Committees are another way to provide direction. Metro established an advisory committee to implement and maintain compliance with PCI

Standards in 2015. Committee members represented several areas of Metro. They included Metro's internal service departments, such as Finance and Regulatory Services and IS, as well as customer-facing departments, like Oregon Convention Center and Oregon Zoo. Including both types of departments helped ensure the need for compliance was considered from diverse perspectives. This approach had the potential to help Metro identify high-risk areas and allocate its resources to address them first.

We found Metro had some policies and guidance to govern cloud computing technology. Policies and guidance can help ensure effective governance by setting clear expectations for employees. Metro's information security policy required IS to approve use of cloud computing technology in writing. Requiring IS involvement in cloud computing decisions increased the chances that security concerns would be considered before finalizing agreements with outside vendors. It also had the potential to reduce duplication of efforts by creating a list of already approved vendors and relying on IS expertise to evaluate risks.

Additionally, in July 2018 Metro developed guidance for the storage of public records and data in the cloud. This guidance described regulatory compliance considerations, and a process to engage Metro's subject matter experts when developing requirements for cloud service providers. Using the guidance could limit Metro's exposure to information security risks. It included a questionnaire to help employees evaluate the vendor's ability to meet Metro's security and compliance needs. Best practices state that an organization should have a good understanding of the quality of the service provider before committing to cloud technology.

Metro lacked governance for surveillance camera usage

Metro needed more strategic direction and oversight to govern surveillance camera usage. There were no committees to make decisions about the cameras, or groups to address problems. Metro had not established any performance measures to monitor the effectiveness of the cameras, such as the number of incidents identified or responded to through their use. Processes and plans for camera usage were also underdeveloped.

Metro's decentralized approach to deploy the cameras contributed to a lack of governance. Departments acquired them independently, which made it difficult to anticipate challenges. They did not work with IS to establish policies and procedures to guide their use. Policies that were in place were site-specific, so they only applied to certain workplaces. This might be appropriate due to operational differences. However, if departments do not share information across departments, they miss opportunities to learn from one another.

Fair Information Practice Principles (FIPPs) are an approach record-keeping agencies can take to maintain fairness, privacy, and security. Local, federal, and global organizations use them to develop policies and procedures governing the use of personal information. FIPPs are considered key

principles for privacy protection in the U.S. They include:

- Specifying and documenting the purpose(s) for using cameras;
- Providing notice where cameras are used;
- Protecting cameras against unauthorized access; and
- Minimizing storage of footage.

We compared Metro policies and procedures to these principles. Our review focused on sites that invested most in Metro's recent security improvements. We found policies and procedures were not established to maintain security, privacy, and fairness. Developing policies and procedures that are consistent with these principles could help Metro protect the cameras and the information they collect from unauthorized use.

Exhibit 4 Policies and procedures for surveillance cameras at Metro sites did not fully address key practices

	Site (estimated number of cameras)			
Criteria	**A (140)**	**B (70)**	**C (39)**	**D (20)**
Specification	○	○	●	●
Notification	○	○	●	●
Protection	○	○	◑	○
Minimization	●	●	●	○

● = *fully addressed* ◑ = *partially addressed* ○ = *not addressed*

Source: Metro Auditor's Office comparison of Metro policies and procedures to Fair Information Practice Principles (FIPPs).

Some sites did not specify or fully document purposes for which the cameras should be used. This created the opportunity for abuse. It also made holding users accountable more difficult. If users do not know how the cameras ought to be used, they could use them improperly. For example, without clear instruction, cameras intended to secure a building could be used to inappropriately monitor employees.

Some sites did not provide notice that cameras were in use. This could give an advantage to those with access to footage, should there be an investigation or dispute. Employees and the public may not know they are on camera at sites where notice is not provided. This has the potential to limit their ability to access footage, which can be used as evidence during accident or incident investigations, or to resolve disputes. If employees or members of the public

that are under investigation or involved in disputes are unaware that footage exists, they may be less prepared to defend themselves.

Documenting access to footage can help protect the cameras from unintended use. None of the sites we reviewed documented a process for granting access, and only one documented which positions had access. Not documenting processes for granting access can also lead to abuse. This may present reputational or legal risks to Metro, if users take unauthorized action, or action based on unauthorized access to footage. At Metro, security and facilities personnel primarily had access, but there were cases where footage was shared with other positions. Some employees could access footage from home, or other sites. In some cases, footage could be viewed by passers-by because it was not in a secure part of the building.

Documented processes for sharing footage can also protect the cameras from unintended use. Only one site had one. This helped ensure footage was only shared for specified purposes, and with those who had authorized access.

In one case, footage was stored longer than Metro's retention schedule. Storing footage longer than necessary increases the risk of unintended use, which may result in reputational damage and customer retention issues for Metro.

Governance was ineffective to comply with Payment Card Industry Standards

Despite having some aspects of best practices in place, efforts to address the risk of noncompliance with PCI Standards have not been successful. The committee Metro established did not have the required information or plans it needed to fulfill its purpose. The committee's design also made it less effective. As a result, compliance with PCI Standards has not been achieved. This elevates the risk that cardholder data breach or theft may occur and could cause Metro and its customers to lose money.

Information was not available to effectively govern. Inconsistent reporting and changing plans made it difficult for the committee to reach a shared understanding of Metro's compliance status. This limited the committee's capacity to advise Metro leadership on what needed to be done. Information about Metro's compliance with PCI Standards was lacking because systems were not in place to provide it. Information to effectively govern the risk of noncompliance with PCI Standards includes performance indicators, assessments, and reports. We found that Metro could:

- **Establish performance indicators to measure compliance with PCI Standards.** National guidance states that information security performance measures should include measures to demonstrate progress in implementing specific security controls, such as PCI Standards. They require data that can be obtained from assessments reports.
- **Conduct assessments against the requirements to comply with PCI Standards.** According to guidance for maintaining payment

security, entities must use official documents from the PCI Security Standards Council to verify their compliance. They are the only acceptable documentation to illustrate compliance with PCI Standards. Forms include templates for outside firms to report compliance based on their assessments, and questionnaires for entities to conduct self-assessments.

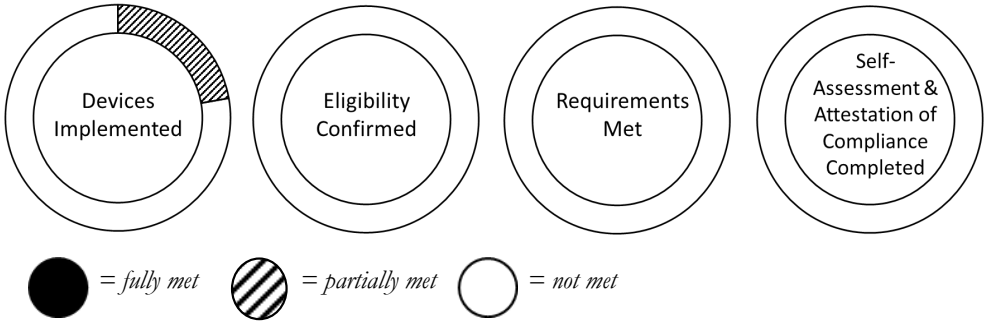
- **Report progress on meeting compliance with PCI Standards.** Compliance with PCI Standards was not reported consistently. Best practices for creating meaningful security metrics show that achievement of requirements to comply with PCI Standards should be reported annually. This allows entities that are not fully compliant to identify steps to remedy their status and targets for compliance. It also helps entities that are fully compliant to maintain compliance.

Metro's initial plan to achieve compliance with PCI Standards was underdeveloped. Plans can help an organization determine its strategic direction. Not including associated costs, clearly designated responsibilities, or timeframes in the plan for compliance reduced Metro's ability to achieve it.

In July 2017, a different approach was announced: implement devices that use a PCI-listed point-to-point encryption solution. This technology makes cardholder data unreadable to an unauthorized party. Putting the devices into use can help Metro reduce the value of stolen cardholder data. It can also make compliance easier for Metro by reducing the scope of data it needs to protect. However, these devices do not remove the need for compliance with PCI Standards entirely.

Under the new approach, there was still significant progress to be made. As of June 2018, the technology had not reached most of Metro. The devices were implemented in four areas. At least 14 areas remained. Metro may qualify to meet fewer requirements for compliance where the devices are used. To qualify, Metro must confirm its eligibility. Once Metro's eligibility has been confirmed, a self-assessment and attestation of compliance must be completed. Additional requirements may apply where the encryption devices are not used.

Exhibit 5 Substantial work remains before Metro meets security standards for payment card data



Source: Metro Auditor's Office analysis based on PCI Standards and June 2018 IS Director's memo to Metro's PCI Advisory Committee.

The design of the committee also contributed to its ineffectiveness. It was created to serve in an advisory capacity, so it lacked authority for decision-making. The committee was required to meet as frequently as needed to complete initial compliance requirements. This provided too much flexibility to achieve its mission. These factors reduced Metro's ability to achieve compliance. A stronger governance structure could overcome these challenges.

Governance of cloud computing would benefit from more thorough contract language

Contracts and agreements are an important component of governing cloud computing technology. This is because they document how services are provided and how information security risks are managed. We reviewed a selection of four cloud computing contracts that were used for ticketing services, event registration, and recruitment. Overall, we found Metro could improve its governance of cloud computing contracts through improved contract language. Doing so would ensure information security risks are addressed and clear performance expectations are included in contracts.

Part of the reason why Metro may have not addressed these risks was because it had yet to develop standard contract language for cloud computing contracts. Another reason was that guidance was only recently created, so there has not been much time to put it into use. We also found that Metro needed to follow its information security policy and develop a long-term plan for cloud computing technology.

The United States Government Accountability Office developed 10 key practices for cloud computing contracts to help ensure services were performed effectively, efficiently, and securely. The key practices were organized into four management areas – roles and responsibilities, performance measures, security, and consequences. We found that Metro adequately addressed roles and responsibilities in the contracts we reviewed, though improvements were needed related to performance measures, security, and consequences.

Exhibit 6 Metro's cloud computing contracts partially met key practices

Criteria	Contract A	B	C	D
Roles & Responsibilities	●	●	●	●
Performance Measures	◑	◑	◑	○
Security	◑	◑	◑	○
Consequences	○	○	○	○

● = *fully met* ◑ = *partially met* ○ = *not met*

Source: Metro Auditor's Office analysis of Metro's cloud computing contracts against key practices.

- **More detail was needed for contract performance measures.** For example, most of the agreements we reviewed ensured Metro had access to its data once the agreement was signed. But, not all of the agreements clearly defined how the data would be transferred back to Metro if the vendor went out of business or the agreement ended. This could present an information security risk because Metro may not have the ability to fully recover its information if the agreement is terminated. It will be important for Metro to include language in future agreements that address this risk.
- **Additional clarity was needed regarding security.** Most of the agreements we reviewed defined who had access to the data stored in the cloud application and what was in place to protect Metro's data. However, not all of the agreements clearly defined how and when Metro would be notified if a data breach occurred. In the absence of language that clearly defines how Metro would be notified, Metro's ability to respond could be limited.
- **Contracts reviewed did not specify enforceable actions for lack of performance.** Key practices indicated that contracts should have language that includes consequences that are specifically linked to contract performance measures. Although Metro had a standard term in its contract that allowed it to withhold payments based on the contractor's performance, it was not specific to any performance measure. For example, if the contract included a performance measure related to the service level for the application, the contract should also include consequences if that service level is not met. Greater specificity could reduce the time it takes to settle disputes related to contractor performance.

In addition, we found that Metro needed to follow its policy related to cloud storage providers. Metro's information security policy stated that the IS department would publish a list of approved cloud storage providers on its webpage. However, the department had not published one. Its webpage stated that the use of cloud storage services was not allowed to save Metro documents and files, but that an approved business cloud storage service would be offered. We were told an approved list was being developed. Doing so could help save time by allowing employees to quickly find vendors that were already vetted. It may also reduce the impact on IS staff resources by consolidating Metro's agreements instead of having multiple agreements with similar or even the same vendors.

Once Metro addresses cloud computing contract language risks, it will be important to review and develop a long-term plan for cloud technology. Adopting cloud computing could help Metro reduce the amount of on-site data storage needed, which could reduce costs. It also could help the agency retain its records in the event of a disaster because the data would not be stored on Metro's premises. Although, this technology presents several opportunities for Metro, it will be just as important to ensure information security risks are addressed through effective contract language.

Recommendations

To improve IT governance, Metro should:

1. Develop a strategic plan
2. Establish a governance structure to oversee its implementation

To improve information security governance, Metro should

3. Develop policies and procedures for surveillance cameras that:
    a. Specify the purpose(s) for which cameras should and should not be used
    b. Ensure notice is provided where cameras are used
    c. Establish processes for granting access and sharing footage
    d. Retain footage consistent with Metro's Records Retention Schedule

4. Take the following actions to comply with PCI Standards:
    a. Implement encryption devices in all areas
    b. Fulfill the requirements for PCI compliance
    c. Develop systems to periodically measure and report on the status of compliance

5. Include language in cloud computing contracts that:
    a. States how and when Metro would be notified of a data breach
    b. Specifies a range of enforceable actions for non-compliance with contract performance measures
    c. Specifies how data would be transitioned back to Metro in the case of contract termination

6. Publish a list of approved cloud storage providers
7. Develop a long-term plan for cloud technology

Scope and methodology

Our 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. We focused our audit on Information Services (IS) and the departments that used these technologies, from July 2012 to November 2018.

We reviewed budget documents related to information security and technology to gain general familiarity with our topic. We also reviewed the mission, strategic plans and performance measures, organizational charts, and written policies and procedures of the IS department. We conducted interviews with managers and staff in IS and other departments to deepen our understanding. We also reached out to Office of Metro Attorney to learn of any ongoing investigations or legal proceedings related to our topic.

We reviewed laws and other requirements to see whether Metro was in general compliance. We identified and assessed major risks, including potential fraud and abuse. We also conducted an historical analysis of IS expenditures, including capital spending.

We reviewed prior Metro audits to determine what actions were taken to address audit recommendations. We also reviewed relevant audit reports from other jurisdictions, and professional literature. In addition, we reviewed employee survey results, and results from an assessment of the IS department.

To determine if Metro followed best practices for information security, we interviewed knowledgeable personnel and reviewed relevant documentation in each area. We conducted interviews with operations management from Portland'5 Centers for the Arts, Oregon Convention Center, and Property and Environmental Services. We reviewed policies, plans, procedures, and performance information, as well as meeting materials. We also reviewed a selection of Metro's contracts with cloud computing application providers.

We identified opportunities for Metro to adhere to best practices using professional literature from:

- World Privacy Forum
- Payment Card Industry Security Standards Council
- Government Finance Officers Association
- Canadian Audit & Accountability Foundation
- National Institute of Standards and Technology
- The Government Accountability Office
- U.S. Department of Homeland Security
- The Office of the Austin City Auditor, Portland Audit Services Division, and County of San Diego Office of Audits & Advisory Services

This audit was included in the FY 2017-18 audit schedule. We conducted this

performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Management response

Memo

Metro
600 NE Grand Ave.
Portland, OR 97232-2736

Date: Thursday, March 7, 2019

To: Brian Evans, Metro Auditor

From: Rachel Coe, Information Services Director
Andrew Scott, Deputy Chief Operating Officer

Subject: Management Response – 2019 Information Services Audit

Management would like to thank the Metro Auditor for reviewing data security in the agency. Ensuring the safety of the information held by Metro is of critical importance. Because public trust is at the heart of Metro's core values, Information Services has sought to make continuous improvements in all areas including redundancy, system and data integrity and security.

Background

The Information Services department at Metro has been making large strides in security over the last few years. While the agency has always protected the network and key systems with firewalls, malware and virus protection, in 2015, Information Services implemented next generation firewalls and service subscriptions to help detect and block application, port and protocol attacks. These intelligent systems receive continuous updates on identified threats, sometimes within minutes of detection, at points around the globe. In 2016, we followed with a full rollout of new security protocols, policies and user awareness notifications. Since then, Information Services has and will continue to add new technologies and security elements to protect our systems and data.

Response to recommendations in the Auditor's report

Management agrees with the overall findings and recommendations.

Recommendations

To improve IT governance, Metro should:

1. *Develop a strategic plan*
2. *Establish a governance structure to oversee its implementation*

Management agrees with the recommendation to develop a strategic plan. As part of that plan, a governance structure for implementation will be included. Funding for a strategic plan was approved in FY 2018-19 and the selection of a contracted firm to help create the plan is currently underway. Management anticipates the effort to begin in late March and will take between four and six months to complete.

To improve information security governance, Metro should:

3. Develop policies and procedures for surveillance cameras that:
   a. Specify the purpose(s) for which cameras should and should not be used
   b. Ensure notice is provided where cameras are used
   c. Establish processes for granting access and sharing footage
   d. Retain footage consistent with Metro Records Retention Schedule

Management agrees with the third set of recommendations. In September 2018 a group of video system stakeholders were brought together to evaluate a change to our standard video recording services. This group will be reconvened to develop a governance plan to implement the recommendations, similar to other agency-wide assets such as SharePoint and Metro's Voice over IP (VoIP) communications system.

4. Take the following actions to comply with PCI Standards:
   a. Implement encryption devices in all areas
   b. Fulfill the requirements for PCI compliance
   c. Develop systems to periodically measure and report on the status of compliance

We agree that Metro should fulfill all of the requirements for PCI compliance and create a method for periodically reporting compliance. On recommendation 4.a, Metro will be conducting a PCI fit/gap assessment during April and May of 2019. That report will indicate where any additional encryption devices are needed.

5. Include language in cloud computing contracts that:
   a. States how and when Metro would be notified of a data breach
   b. Specifies a range of enforceable actions for non-compliance with contract performance measures
   c. Specifies how data would be transitioned back to Metro in the case of contract termination

Management agrees with the majority of the recommendations for cloud computing. Information Services has been working with the Metro Attorney's office on template language to be included in technology contracts, specifically with cloud contracts. Information Services will follow up with both the Metro Attorney's office and Finance and Regulatory Services to get the changes implemented. It should be noted that the department's ability to implement such language will be dependent upon acceptance by our vendors.

6. Publish a list of approved cloud storage providers
7. Develop a long-term plan for cloud technology

We agree with recommendations six and seven. Information Services is currently updating its Intranet presence and will include approved cloud providers on the list. Part of the requirements for the IS strategic planning project is development of a five-year cloud strategy. This should be available by the end of the calendar year.

We want to thank the Auditor again for reviewing this topic and helping to emphasize the importance of technology in the agency and the need to create a secure environment for our information.

Office of the Metro Auditor
600 NE Grand Avenue
Portland, Oregon 97232
503-797-1892
www.oregonmetro.gov