May 9, 2018

Honorable Mayor and Members of the City Council:

Enclosed is the audit report for *Intelligent Transportation Systems*, which was included on the Council-approved FY 2017/18 Audit Plan as a contracted information technology audit. We contracted with Grant Thornton LLP, to perform an evaluation of the City's Intelligent Transportation Systems' (ITS) general and application controls.

The audit found that risks surrounding ITS have not been adequately identified, evaluated and managed. Specifically, the Traffic Management Center (TMC) should take a more proactive role in managing security risk; establish stronger access controls to protect TMC computers, servers, and applications; and develop business continuity and disaster recovery plans. Additionally, few policies and procedures have been formalized, and vendor service agreements have not been properly maintained and managed. Overall, strategic planning and additional performance data may help ITS more effectively plan for future improvements.

If you need additional information or have any questions, please contact me at (480) 312-7867.

Sincerely,

Sharron Walker

Sharron E. Walker, CPA, CFE, CLEA
City Auditor

Audit Team:

Lai Cluff, CIA – Sr. Auditor
TABLE OF CONTENTS

AUDIT HIGHLIGHTS .................................................................................................................................................. 1

BACKGROUND ........................................................................................................................................................ 3

Figure 1. Traffic Management Center (TMC) Organizational Structure .............................................................. 3
Figure 2. TMC ........................................................................................................................................................ 4
Figure 3. TMC Operating Expenditures and Approved FTE, FYs 2012/13 - 2016/17 ........................................... 4
Figure 4. Video Detection Camera and Controller Cabinet .................................................................................... 5

OBJECTIVES, SCOPE, AND METHODOLOGY .................................................................................................. 7

Figure 5. COBIT® 5 Assessment Framework ......................................................................................................... 7

FINDINGS AND ANALYSIS ................................................................................................................................. 9

1. Risks surrounding Intelligent Transportation Systems (ITS) have not been adequately identified, evaluated and managed.................................................................................................................................... 9

2. Several areas in IT governance and management could be improved. ......................................................... 11

Figure 6. Capital Expenditures for ITS and Signals Projects ............................................................................... 13

MANAGEMENT ACTION PLAN .......................................................................................................................... 15
AUDIT HIGHLIGHTS
Intelligent Transportation Systems

WHY WE DID THIS AUDIT

An audit of Intelligent Transportation Systems was included on the City Council-approved fiscal year (FY) 2017/18 Audit Plan as a contracted information technology (IT) audit. We contracted with Grant Thornton, LLP, to perform an evaluation of Intelligent Transportation Systems' general and application controls.

BACKGROUND

Scottsdale's Traffic Management Center (TMC), within the Street Operations department of the Public Works division, manages the Intelligent Transportation Systems (ITS).

According to the U.S. Department of Transportation, these systems include a variety of technologies applied to monitor, evaluate, operate, and manage transportation systems to enhance efficiency, reliability, and safety.

The TMC indicated approximately 77% of the City's 305 signalized intersections are currently connected to the ITS through 175 miles of fiber optic cables and 90 ethernet radios. The ITS Traffic Engineer periodically evaluates and adjusts signal timing using a transportation management software.

WHAT WE FOUND

Risks surrounding ITS have not been adequately identified, evaluated and managed.

The TMC does not have a documented risk management process, and it is not otherwise apparent that potential risks have been adequately assessed.

Specifically, we found:

• The TMC should take a more proactive role in managing security risks, including working with the City's central IT department to better define roles and responsibilities over security management.
• Stronger access controls are needed to protect TMC computers, servers, and applications from unauthorized access.
• Business continuity and disaster recovery plans have not been established.

Several areas in IT governance and management could be improved.

We found:

• Few policies and procedures have been formalized, making knowledge transfer among staff more difficult and potentially inconsistent.
• Vendor service agreements have not been properly maintained and managed. In two instances, no written agreements exist.
• Strategic planning and additional performance data may help ITS more effectively plan for future improvements.

WHAT WE RECOMMEND

We recommend the Traffic Management Center:

• Work with the IT department to review roles and responsibilities for technology management activities.
• Formalize policies and procedures for TMC operations and establish stronger access controls over the TMC systems.
• Ensure written agreements are established and software acquisitions follow the procurement review process.
• Identify and assess potential risks and develop business continuity and disaster recovery plans.
• Develop a strategic plan to guide TMC operations and ITS objectives.

MANAGEMENT RESPONSE

The Department agreed with the recommendations.
BACKGROUND

This audit of *Intelligent Transportation Systems* was included on the City Council-approved fiscal year (FY) 2017/18 Audit Plan as a contracted information technology (IT) audit. We contracted with Grant Thornton, LLP, to perform an evaluation of Intelligent Transportation Systems’ general and application controls.

Scottsdale’s Traffic Management Center (TMC), within the Street Operations department of the Public Works division, manages the Intelligent Transportation Systems (ITS). The ITS Manager along with an ITS Traffic Engineer, an ITS Analyst, 2 ITS Operators, a Network Technician, and an ITS Traffic Engineer Analyst staff the TMC. In addition, 10 signal technicians assigned to signal maintenance or construction support the TMC operations.

**Figure 1. Traffic Management Center (TMC) Organizational Structure**

*SOURCE:* Department organization chart, April 2018.
Key ITS stakeholder groups within the City include the Transportation and the Police departments. Transportation (within the Community & Economic Development division) staff plans and engineers the City’s physical transportation infrastructure. They also plan and obtain funding for some ITS projects and use ITS data for traffic analysis to evaluate future transportation needs. Certain Transportation and Police staff have access to view the traffic cameras’ live video feeds. The Police Department may also work in the TMC to monitor and adjust traffic flow during large special events and police emergencies.

In 2014, the TMC moved from its previous location in the Transportation suite of the One Civic Center building to an updated center at the North Corp Yard. The new center includes a video wall for monitoring traffic cameras, as shown in Figure 2, as well as upgraded equipment. Figure 3 summarizes the TMC’s operating expenditures for the ITS and Traffic Signals cost centers and its approved full-time equivalents (FTE) over the past five fiscal years.

Figure 3. TMC Operating Expenditures and Approved FTE, FYs 2012/13 - 2016/17

SOURCE: Auditor analysis of departmental budget reports for ITS and Traffic Signals cost centers.
Intelligent Transportation Systems

According to the U.S. Department of Transportation, Intelligent Transportation Systems (ITS) include a variety of technologies applied to monitor, evaluate, operate, and manage transportation systems to enhance efficiency, reliability, and safety. Further, ITS can encompass all modes of transportation, including pedestrian, vehicle, bicycle and public transit.

Data communication is critical to an ITS, as connectivity between the traffic signals and devices to the TMC allows staff to monitor and control traffic operations from a centralized location. According to the department, approximately 77% of the City’s 305 signalized intersections are currently connected to the TMC through 175 miles of fiber optic cables and 90 ethernet radios. Other necessary equipment includes the pan/tilt/zoom (PTZ) cameras, video detection cameras and controller cabinets. The ITS Traffic Engineer periodically evaluates and adjusts signal timing using TransSuite, the transportation management software by TransCore. The TMC staff also uses this software to control traffic signals in real time for response to incidents, construction work zones or other issues impacting traffic flow.

As well, the City primarily uses three different methods of vehicle detection to adjust signal timing for increased traffic.

- **Loop detection** uses an inductive loop laid in the asphalt to detect vehicles as they pass through or stop within the loop’s magnetic fields. While loop detection is reliable and slightly less expensive, it can be damaged by street pavement or construction work.

- Since 2015 the City has updated nearly a third of its intersections to **video detection**. As shown in Figure 4, these cameras are installed on the traffic signals to detect vehicles as they approach or stop within the detection zones designated by the TMC. Video detection cameras have been configured to also detect activity in the bicycle lane. The Street Operations department plans to eventually transition all intersections to video detection.

- In addition, the Loop 101 interchange at Frank Lloyd Wright Boulevard uses **radar detection**. This technology detects vehicles further up the ramp.

As part of a federally-funded regional project along Frank Lloyd Wright Boulevard, between Scottsdale Road and Thompson Peak Parkway, the TMC manages signal timing using Adaptive Signal Control Technology (ASCT). This system, also managed through the TransCore application, continuously gathers data from the corridor’s traffic detectors (including the radar detectors) and makes real-time
signal timing adjustments to improve traffic flow. The City implemented this system in partnership with the Maricopa County Department of Transportation as part of a larger Bell Road Project.\(^1\) According to the TMC, Scottsdale implemented the new system in August 2017, and complete results of the adaptive system’s impact on traffic congestion are not yet available.

\(^1\) Bell Road, which becomes Frank Lloyd Wright Boulevard in Scottsdale, also stretches across the cities of Phoenix, Glendale, Peoria and Surprise.
OBJECTIVES, SCOPE, AND METHODOLOGY

An audit of Intelligent Transportation Systems was included on the City Council-approved fiscal year (FY) 2017/18 Audit Plan as a contracted information technology (IT) audit. The audit objective was to evaluate the effectiveness of IT controls over the City’s Intelligent Transportation Systems (ITS).

We contracted with specialists from Grant Thornton, LLP, to assist with the technical review of ITS general and application controls. As required by Government Auditing Standards, we evaluated the qualifications and independence of the specialists and documented the nature and scope of the specialists’ work, including the objectives and scope of work, intended use of the specialists’ work to support the audit objectives, and the specialists’ procedures and findings.

To achieve the audit objectives, the Grant Thornton specialists evaluated the ITS department based on COBIT® 5 standards for governance and management of enterprise IT, summarized in Figure 5.

Figure 5. COBIT® 5 Assessment Framework

To gain an understanding of the Traffic Management Center’s (TMC) policies and practices related to the ITS, the audit team (Grant Thornton specialists and City Auditor staff) interviewed the ITS Signals Manager, the Lead ITS Analyst, the ITS Network Technician, and the ITS Traffic Engineer. The audit team also interviewed the IT Director and Chief Information Security Officer in the City’s central IT department to gain an understanding of the IT department’s role with the ITS.

To evaluate the effectiveness of IT controls, the audit team reviewed the TMC’s work order system, policies and procedures, vendor contracts, TransCore system user and change reports, and performance metrics. Further, the audit team observed the TMC’s physical location and security in operation.

The audit found that risks surrounding ITS have not been adequately identified, evaluated and monitored. The department should take a more proactive role in managing security risk and needs to establish stronger access controls over its workstations, servers and applications. Additionally, business continuity and disaster recovery plans need to be developed. Other areas of IT governance and management that need improvement include: development of formal policies and procedures, management of vendor agreements, and strategic planning.

We conducted this audit in accordance with generally accepted government auditing standards as required by Article III, Scottsdale Revised Code §2-117 et seq. 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. Audit work took place from September 2017 through March 2018.
FINDINGS AND ANALYSIS

1. Risks surrounding Intelligent Transportation Systems (ITS) have not been adequately identified, evaluated and managed.

Information Technology risk management typically encompasses risk assessment, risk mitigation, and ongoing risk evaluation and assessment. The Traffic Management Center (TMC) does not have a documented risk management process and it is not otherwise apparent that potential risks have been adequately assessed. Key risk areas for TMC may include technical/IT risks and external risks, such as natural disasters and other uncontrollable events.

A. The TMC should take a more proactive role in managing security risk.

The TMC’s communications network is separated from the City’s network. The City’s central IT department manages the network and firewall for the TMC’s network. However, it does not manage or provide oversight for the computers, applications, equipment and devices within the TMC’s network. This separation in IT management leaves some gaps in management of enterprise risk.

For example, the TMC relies on the central IT department to manage its network and firewall security and does not proactively engage in managing those security risks. External access for vendors and employees into the TMC network must be requested through IT department’s work order system and provided by its security staff. However, once provided, the TMC does not periodically review the provisioned users to ensure continued access is still needed.

Additionally, the TMC has not conducted security assessments to evaluate potential network vulnerabilities or cybersecurity threats. The IT department performs routine vulnerability scans on the City network but has not included the TMC network in these scans. As well, there is some uncertainty as to whether the controller cabinets represent an access risk.

B. Access controls for the ITS applications need improvement.

TMC staff manage user access to the computer workstations and ITS applications within the TMC network. However, the department does not have policies or procedures to govern user access, and current practices do not reduce the risk of unauthorized access.

- The computer workstations and applications running on them were generally open and accessible to anyone within the center. All TMC staff use the same workstation login credentials.
- While the TransCore signal management system requires a separate login, there are several generic user (not specific to an individual) and vendor support accounts, as well as one account for a recently terminated employee. All these accounts have high levels of access privileges, including the right to make changes.
- Although it is a standard IT practice, the TMC does not require system passwords to be changed periodically or when employees leave TMC employment.

These practices increase the risk of unauthorized changes to the signal controls using accounts that are not easily traceable to an individual.
It appears the shared access was established to allow multiple staff to monitor traffic cameras shown on the display wall throughout the day and also make any necessary signal adjustments. If shared user accounts cannot be eliminated, their access privileges should be limited to view-only. Making system changes should require individual login credentials. Further, other applications running on the TMC workstations should also require individual logins and not be available through the shared accounts.

Currently, physical security is the primary barrier to accessing the ITS applications that are running on TMC workstations. The TMC has several doors that are accessed using employee badges. In addition to computer workstations, the TMC houses some application servers, which are also accessible to anyone that enters the center. The department should establish internal policies for physical security, such as requiring that doors are not propped open, computers are logged off when employees leave, and access to the server area is restricted.

C. Business continuity and disaster recovery plans have not been established.

The Street Operations department recently started the business continuity planning process with the City’s Emergency Management staff. The TMC is working to identify its critical services and how to continue to provide those services in the case of a disruptive event. However, according to the Emergency Management staff, this process will not encompass disaster recovery for IT systems.

The TransCore applications housed on servers at the City data center are backed up routinely, but other applications located on TMC servers are not backed up. The IT department is currently setting up a co-location facility to provide redundancy of critical IT services. This will include the TransCore system servers that are physically located in the IT data center. However, the TMC still need to evaluate the potential risks should an event disrupt ITS operations at its own location. Having a recovery plan in place can minimize the potential impact on citizens.

Recommendations:

The Traffic Management Center should:

A. Work with the IT department to review roles and responsibilities for technology management activities, identify potential security risks and options for minimizing those risks. In particular, the TMC should request that the IT network vulnerability scans include the ITS network and devices.

B. Establish policies and procedures relating to TMC physical and user access to workstations, servers and applications to minimize the risk of unauthorized changes or disruptions.

C. Identify and assess potential risks and create a plan to reduce those risks, including developing business continuity and disaster recovery plans.
2. Several areas in IT governance and management could be improved.

Several key areas in IT governance and management could be improved, including documenting policies and procedures, managing vendor agreements and performance, and establishing strategic objectives and plans.

A. Few policies and procedures have been formalized, making knowledge transfer among staff more difficult and potentially inconsistent.

Our audit specialists observed that the TMC is fairly mature in practice and can meet its day-to-day operational needs. However, they also noted that critical information about the ITS network, infrastructure, and configuration is known by a few key individuals, and operations may be impacted should any of these individuals abruptly leave.

The department acknowledges the potential risk and has begun formalizing more of its policies and procedures. In addition to traffic signal design standards included in the City’s Design Standards & Policies Manual, the TMC has basic signal timing policies and set-up procedures for video detection. But information such as network architecture, device configuration standards, equipment maintenance, and emergency procedures has not yet been adequately documented.

B. Vendor service agreements have not been properly maintained and managed.

1) For the primary technology vendor, TransCore, the TMC has been using an expired contract. Further, the TMC has not significantly updated the service agreement since 2009. Typical service-level measures, such as downtime limits, maintenance windows, and issue response time, are not stipulated in the service agreement. As well, TMC staff do not know what the vendor’s software update process is and whether updates are adequately tested prior to installation onto the TMC’s live system.

2) The TMC does not have written agreements for some vendor-supported software services and did not consistently follow established purchasing and IT review processes when acquiring new software. In particular, for Software as a Service (SaaS) applications, where the vendor may provide application hosting, data storage and/or data processing, the contract is typically reviewed by the IT department, Risk Management, and the City Attorney’s office for compatibility with City technology and data security, liability, and legal requirements. At least two applications did not have written agreements, so they did not go through the typical purchasing and IT review process.

- One application, purchased several years ago through a change order on an engineering services contract, collects travel time data. The TMC staff use this mobile application periodically to collect travel time data on selected City streets and store it on the vendor’s cloud service. While this data may represent low risk in terms of privacy, there is no written agreement to govern the use, retention and storage of the data.

- The second application uses signal timing data to provide data analytics. According to the TMC, the software service is under development and was provided free of charge on a pilot basis. There is no written agreement, but it appears the vendor was allowed to test its service on the TMC’s equipment and server. There is no additional documentation available and it is not clear how much access the vendor was given to

---

2 The City’s DS&PM provides guidance for development projects within Scottsdale.
the TMC systems or exactly what data is extracted. Allowing a third-party direct access to the traffic systems and the City's data should be reviewed closely for potential security concerns and data ownership and privacy. Additionally, although the vendor provided the application free of charge on a pilot basis, the vendor’s stated goal is to eventually sell software services to the City. The City’s purchasing policies generally do not allow departments to accept free products for testing or trial outside of the structured procurement process.

The IT and legal contract review requirements are typically triggered by the purchasing process. In both instances, the TMC did not follow the usual procurement processes.

C. Strategic planning and additional performance data may help ITS more effectively plan for future improvements.

The TMC does not have a strategic plan to outline its short-term and long-term objectives and strategies for achieving those objectives. Strategic planning documents need to exist which outline the department’s strategy, identify business outcomes, and define how the organization manages to this on a day to day basis. An ITS strategic plan, aligned with the Transportation Master Plan, may help provide a vision for Scottsdale’s future ITS.

Decisions regarding capital projects and improvements should be made with strategic objectives in mind. Approved capital budgets for ITS and signal improvement projects totaled about $1.8 million for FY 2017/18. Figure 6 on page 13 shows actual capital expenditures for the last 5 fiscal years for ITS-specific projects. As well, strategies and decision making should be data-driven. Specifically, the audit found that:

- Cost-benefit of new tools and technology has not been evaluated. Evaluating the short-term and long-term cost of new equipment or technology, such as upgrading fiber cables or installing new devices, in comparison to their potential benefits would assist in prioritizing investment decisions.

- Additional data-driven performance metrics can help anticipate future system requirements. Currently, the department’s primary performance objective is to improve the travel time in certain corridors by 10%. Additional measures tied to strategic goals may provide better data regarding the department’s day-to-day performance and provide more context for decision making.

- Documentation of the ITS network and architecture is incomplete. Having complete and accurate information is necessary for strategic decision-making and long-term planning. The department has begun the process of mapping its fiber network.

- Improved asset management practices are needed. Documentation of asset inventories did not specifically identify the asset (by serial number or similar means) to ensure accountability for purchased assets. Stored equipment and other non-network devices were also not included on asset listings. In addition to maintaining a complete asset list, tracking other information, such as the acquisition date, installation date, repair issues and estimated useful life, may help the TMC to plan for future replacement costs and request warranty repairs when applicable.

---

3 Non-network devices are installed devices that do not directly connect to the TMC network.
Figure 6. Capital Expenditures for ITS and Signals Projects

Note: Amounts do not include ITS/Signal projects incorporated into larger Transportation projects.

SOURCE: Auditor analysis of SmartStream reports.

Recommendations:

The Traffic Management Center should:

A. Develop and document policies and procedures, such as standard operating procedures for TMC operations, adopted industry standards and documentation of network architecture.

B. Ensure formal agreements are established and monitored, including service level expectations such as downtime limits, maintenance windows, issue response time. Also, the TMC should follow the City’s established procurement review processes for all new applications.

C. Develop strategic planning documents to clearly identify objectives, outcomes, and strategies to guide TMC day-to-day operations and ITS long-term objectives.
MANAGEMENT ACTION PLAN

1. **Risks surrounding Intelligent Transportation Systems (ITS) have not been adequately identified, evaluated and managed.**

**Recommendations:**

The Traffic Management Center should:

A. Work with the IT department to review roles and responsibilities for technology management activities, identify potential security risks and options for minimizing those risks. In particular, the TMC should request that the IT network vulnerability scans include the ITS network and devices.

B. Establish policies and procedures relating to TMC physical and user access to workstations, servers and applications to minimize the risk of unauthorized changes or disruptions.

C. Identify and assess potential risks and create a plan to reduce those risks, including developing business continuity and disaster recovery plans.

**MANAGEMENT RESPONSE:** Agree

**PROPOSED RESOLUTION:**

A. This will be part of the operations plan.

B. This work is currently in progress.

C. Currently in development with BOLD Planning under Emergency Operations Plan.

**RESPONSIBLE PARTY:** Randy Ghezzi, Public Works Department Director - Street Operations

**COMPLETED BY:** 12/31/2018

2. **Several areas in IT governance and management could be improved.**

**Recommendations:**

The Traffic Management Center should:

A. Develop and document policies and procedures, such as standard operating procedures for TMC operations, adopted industry standards and documentation of network architecture.

B. Ensure formal agreements are established and monitored, including service level expectations such as downtime limits, maintenance windows, issue response time. Also, the TMC should follow the City’s established procurement review processes for all new applications.

C. Develop strategic planning documents to clearly identify objectives, outcomes, and strategies to guide TMC day-to-day operations and ITS long-term objectives.

**MANAGEMENT RESPONSE:** Agree
PROPOSED RESOLUTION:

A. Policies and Procedures are currently being developed using national standards as well as other similar size city standards as benchmarks.

B. Our Team is currently in contact with TransCore and other cities to establish guidelines in a new contract.

C. TMC staff will develop a strategic plan that aligns us with our goals and objectives for the TMC now and into the future.

RESPONSIBLE PARTY: Randy Ghezzi, Public Works Department Director – Street Operations

COMPLETED BY: 12/31/2018
The City Auditor’s Office conducts audits to promote operational efficiency, effectiveness, accountability and integrity.