COUNTY AUDIT DEPARTMENT

REPORT # 373

An Audit of:

MOBILE DEVICE MANAGEMENT

NOVEMBER 26, 2019

Pat Frank INTEGRITY. TRANSPARENCY. ACCOUNTABILITY.

CLERK OF COURT & COMPTROLLER • HILLSBOROUGH COUNTY, FLORIDA

November 26, 2019

The Honorable Lesley "Les" Miller, Jr., Chairman
The Honorable Ken Hagan
The Honorable Pat Kemp
The Honorable Sandra L. Murman
The Honorable Kimberly Overman
The Honorable Mariella Smith
The Honorable Stacy R. White

Dear Chairman Miller and Commissioners:

The Audit Team performed an audit of the Mobile Device Management (Audit Report #373, dated November 26, 2019). No responses were required from the Information and Innovation Office's Director of Technology as the Audit Team did not identify any material concerns.

The purpose of this Report is to furnish management independent, objective analysis, recommendations, counsel, and information concerning the activities reviewed. It is not an appraisal or rating of management.

Although the Audit Team exercised due professional care in the performance of this audit, this should not be construed to mean that unreported noncompliance or irregularities do not exist. The deterrence of fraud and/or employee abuse is the responsibility of management. Audit procedures alone, even when carried out with professional care, do not guarantee that fraud or abuse will be detected.

The Audit Team appreciates the cooperation and professional courtesies extended to the auditors by the Directors and personnel of the IT Infrastructure and Technical Support Department for this audit.

Sincerely,

Heidi Pinner, CIA, CISA, CFE, CRMA
Director of County Audit

CC: Mike Merrill, County Administrator
Ramin Kouzehkanani, Chief Information & Innovation Officer
Kevin Kerrigan, Director of Technology of the IIO
Kevin Brickey, Director, Management & Budget Office
Dan Klein, Chief of Staff, Clerk of Court and Comptroller
Rick VanArsdall, Chief Deputy, Clerk to the Board

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND INFORMATION

Hillsborough County business units provide employees with mobile devices (cell phones and tablets) for their business communication needs. The County's Mobile Device Management (MDM) Team within the Information and Innovation Office (IIO) is in charge of managing these County owned mobile devices. There are currently more than 2,500 devices being managed by the MDM team. The MDM Team uses a platform called AirWatch to manage the network of mobile devices and to govern the security controls of each device. The MDM team also utilizes a system called Smarsh to track and maintain a record of all mobile text communications in compliance with Florida Statutes, Chapter 119, Public Records Law. Mobile devices referenced in this report are iPhones and iPads that are ordered though the County's main cellular communication provider.

OBJECTIVE

The objective of the audit was to determine whether or not there are appropriate controls in place for the purchase and use of County owned mobile devices.

SCOPE

The audit was conducted in conformance with the *Generally Accepted Government Auditing Standards* and the *International Standards for the Professional Practice of Internal Auditing*. These Standards require that County Audit plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit comments and conclusions based on the audit objectives. County Audit believes that the evidence obtained provides this reasonable basis.

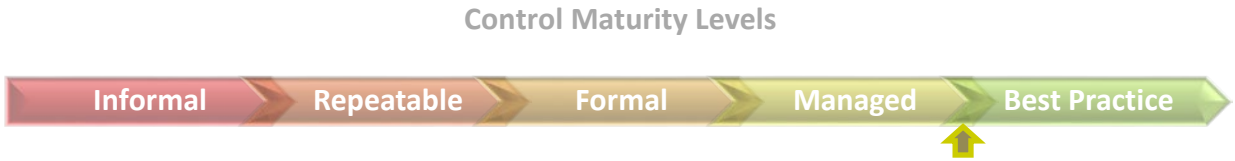
This audit included controls and monitoring activities for County owned mobile devices from October 1, 2018 through February 8, 2019.

OVERALL EVALUATION

The Audit Team did not identify any material concerns that require management's corrective action. Management has adequate controls in place for mobile device management; including:

- Systems to ensure the appropriate designation, management and use of mobile devices.
- Effective deployment of mobile device security policies and controls.
- Record retention controls which comply with County policy and state regulations.
- Controls to restrict the use of applications (APPS) across the network of County mobile devices.

OPINION



The control environment relative to the purchasing, use and record retention process of mobile devices is at a managed maturity level. This is an above average control rating which indicates that established controls are defined and documented, control awareness exists and potential control gaps are detected and remediated timely. This level of control maturity provides greater reliance on prevention versus detection controls and the chain of accountability is well understood.

The exit conference was held on November 20, 2019.

Some minor concerns not included in this Report were communicated to management and/or corrected during fieldwork.

AUDITED BY

Heidi Pinner, CIA, CISA, CFE, CRMA, Director of County Audit
Margaret Brown, CIA, Audit Manager
Raul Cardona, CIA, CISA, CAMS, Senior Internal Auditor

AUDIT COMMENTS & RECOMMENDATIONS

AUDIT COMMENT 1

Adequate controls are in place for the acquisition, management and use of County owned mobile devices.

Mobile Device User Accounts Testing

The Audit Team obtained a population as of February 2019 of 2,051 County mobile devices and their assigned users and determined whether or not controls were in place to ensure that:

a. Each account contained a unique record identifier.

b. Every account belonged to an active employee.

c. The use of test, service or generic accounts was limited and appropriate.

d. System administrator accounts were appropriate based on employee active status, department and position.

e. Mobile devices were properly assigned to users and returned back to the MDM department when an employee separated from the County.

f. A process was in place to identify mobile devices that are being used outside of the monitoring platforms.

Results of Testing

For the 2,051 mobile devices in the population, the Audit Team determined that:

a. Each mobile device record has a unique asset number and phone number assigned.

b. Ninety-nine percent of the devices (2,041 out of 2,051) were assigned to active County active employees. The other 10 devices were assigned to terminated employees.

c. Specific users were assigned to 1,780 (87%) of these devices. There were 265 (13%) generic accounts and 6 (0.3%) test accounts. Generic accounts are utilized by departments such as Fire Rescue and Public Works which have a business need for multiple users to utilize a single device. Test accounts were used only by IIO to perform testing. The Audit Team confirmed that security controls and procedures are applied to these generic and test mobile accounts.

d. There were five (5) active administrator accounts which were all appropriate based on the administrator active status, department and position.

e. The MDM Team assigns devices based on the information included in the STATS (System, Technology and Ticket Support) ticket submitted by the employee's manager. There were a total of 10 mobile accounts from a population of 2,051 (0.49%) that were still assigned to ex-employees at the time of testing. It is the responsibility of the manager to put in a STATS ticket for the IIO to terminate the employee systems access, including deactivating, reassigning or returning applicable mobile devices. Therefore, the MDM team depends on managers to process employee separations on a timely manner in order to have mobile devices properly returned back to them.

   The MDM Team does also perform a quarterly review of devices shown as inactive for more than 120 days and follows up with the respective department directors requesting them to either connect the device to the network or to return it back to the MDM Team.

f. Currently, there's no process or tool available to track mobile devices being used for business outside the AirWatch and Smarsh platforms. Therefore, employees could use an unregistered mobile device for business purposes and MDM would not have the ability to impose security or record retention controls. To mitigate this risk the mobile device policy prohibits the use of unregistered devices and network security controls prevent these devices from connecting to the network.

RECOMMENDATION

The Audit Team did not identify any material concerns that require management's corrective action.

AUDIT COMMENT 2

Management has adequate security controls in place over mobile devices and mobile device information. In addition, record retention procedures are in compliance with policy and regulations.

Mobile Device Security Controls

Security controls for all mobile devices in the County are activated and managed by the MDM team through the AirWatch system. To test the functionality and effectiveness of these security controls, the Audit Team utilized a test phone (provided by the MDM team) and determined whether or not adequate controls were in place to ensure that:

a. A password was required to unlock the phone and the passcode requirement could not be overridden on the device.

b. Failed login attempts resulted in a device lock-out.

c. The device could be locked remotely by the MDM team.

d. The device data could be remotely wiped by the MDM team.

e. The device could be remotely located by the MDM team and the GPS capability could not be overridden on the device itself.

f. The iMessage capability was appropriately restricted so that users cannot circumvent record retention controls.

g. Mobile device data phone data could not be obtained through common mobile device management and data transfer applications (iTunes and Syncios.)

Results of Testing

a. Immediately after password creation, access to the phone was restricted until the correct password was entered.

b. The test phone locked itself after ten consecutive wrong password attempts and increased the lock out interval exponentially with additional attempts.

c. The Audit Team was able to lock the phone remotely utilizing the security feature in AirWatch and this remote lock occurred immediately.

d. The Audit Team was also able to initiate a remote data wipe and reset utilizing the AirWatch system. This remote wipe initialized immediately.

e. The Audit team was also able to locate the device immediately utilizing the monitoring tools.

f. All attempts by the Audit Team to use Apple's iMessage function and circumvent record retention controls failed. The test device could not send or receive iMessages. All text communications performed were received as regular SMS/MMS texts, and subsequently tracked by the Smarsh system.

g. The Audit Team was able to connect the test phone and sync (copy) the information saved in the device to mobile device management and data transfer applications (iTunes and Syncios). However, in order to do so the device password was required before it would allow the syncing process to occur. This mitigating control is adequate to ensure that the information in the mobile device is kept secure by enforcing the password controls.

Additional Mobile Device and Record Retention Testing

The Audit Team selected a random sample of 40 active mobile devices from the population of 2,051 and performed testing to determine whether or not:

a. Each device was acquired in accordance with the current purchasing policy.

b. All applicable security policies were active and monitored.

c. Each device was registered and actively monitored through the Smarsh system.

d. Records of communications were maintained in compliance with County policy and State law. (This test was performed on a sub-sample of 20 mobile devices.)

e. A mechanism was in place to record and maintain mobile device voicemails.

Results of Testing

a. Record of the device acquisition was available for 17 (43%) of the devices in the sample. The remaining 23 devices did not have information to support their initial acquisition and may have pre-dated the existing process (implemented in 2018). As a result, the Audit Team could not determine the effectiveness of the acquisition controls however, the control design appears adequate.

b. All active mobile devices in the sample had the appropriate security policies in place.

c. All active devices in the sample capable of sending or receiving text messages were actively registered in the Smarsh system for records retention.

d. Supporting documentation was maintained and available for the text communications of the 20 devices sampled. This information included the time of communication, text message content, third party number, and attachments. The audit team confirmed that text communications were being captured and maintained for the devices over time but could not confirm the completeness of the records maintained.

e. The County does not currently have the ability to automatically track and store mobile device voice messages. Per the mobile device policy, it is the user's responsibility to forward any business communications received via voice message on a County owned mobile device to their work email or land-line phone. The audit team did not confirm user's compliance with this policy.

RECOMMENDATIONS

The Audit Team did not identify any material concerns that require management's corrective action.

AUDIT COMMENT 3

Management has adequate controls in place over the approval and use of mobile device applications across the network of County mobile devices.

Testing of Mobile Applications

The Audit Team obtained a list of all mobile applications available for County mobile devices, selected a judgmental sample of 10 applications to ensure that:

a. A request to use the application was properly completed.
b. A business need was demonstrated for the use of the mobile application.
c. Proper approval was given prior to application download, installation or use.

Results of Testing

All the applications (100%) had requests properly completed and maintained. Each request clearly established a business need and all applications were reviewed and properly approved by Network Administrators of the IIOMDM Team.

RECOMMENDATIONS

The Audit Team did not identify any material concerns that require management's corrective action.