Mecklenburg County
Department of Internal Audit

Information Technology
Mobile Device Inventory Management
Report 1662

December 18, 2018

Internal Audit's Mission	To support key stakeholders in cultivating an environment of accountability, transparency, and good governance.
Internal Audit Contacts	Joanne Prakapas, CPA/CFF, CIA, CRMA, CFE, Audit Director (980) 314-2889 or joanne.prakapas@mecklenburgcountync.gov Christopher Waddell, CIA, CRMA, Audit Manager (980) 314-2888 or christopher.waddell@mecklenburgcountync.gov
Staff Acknowledgements	Deborah Caldwell, CIA, CISA, Auditor-in-Charge
Obtaining Copies of Internal Audit Reports	This report can be found in electronic format at http://mecknc.gov/audit/reports/pages/default.aspx

MECKLENBURG COUNTY
Department of Internal Audit

To: Keith Gregg, Chief Information Officer, Information Technology Services
Mark Hahn, Director, Asset and Facility Management

From: Joanne Prakapas, Director, Department of Internal Audit

Date: December 18, 2018

Subject: Mobile Device Inventory Management Report 1662

The Department of Internal Audit has completed its audit of mobile device inventory management processes to determine whether internal controls effectively manage key business risks inherent to this activity. Internal Audit interviewed key personnel; reviewed and evaluated policies, procedures, and other documents; observed operations; and tested various mobile device inventory activities from July 1, 2012 through October 30, 2017. Mobile device configuration was excluded from this review.

This audit was conducted in conformance with The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. These 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.

OVERALL EVALUATION

Overall, key risks inherent to mobile device inventory management were not managed to an acceptable level, and opportunities exist to improve the design and operation of key control activities.

RISK OBSERVATION SUMMARY

The table below summarizes the risk observations identified during this audit, grouped by the associated risk factor, and defined in Appendix A. The criticality or significance of each risk factor, as well as Internal Audit's assessment of the design and operation of key controls to effectively mitigate the risks, are indicated by the color codes described in Appendix B.

RISK OBSERVATION SUMMARY			
Risk Factors and Observations	**Criticality**	**Design**	**Operation**
1. Policies and Procedures Risk	🔴	🔴	🔴
1.1 Department Formal Documentation (ITS) 1.2 Department Formal Documentation (AFM) 1.3 Enterprise Formal Documentation			
2. Existence Risk	🔴	🔴	🔴
2.1 Asset Management			
3. Physical Security Risk	🟡	🟡	🟡
3.1 Physical Access			
4. System Access Risk	🔴	🔴	🔴
4.1 Logical Access			
5. Segregation of Duties Risk	🔴	🟡	🟡
5.1 Mobile Device Procurement			
6. Compliance Risk	🔴	🟢	🟡
6.1 Process Execution			
7. Accounting Risk	🟡	🟢	🟢
No Risk Observations Noted			

The risk observations and management's risk mitigation strategies as defined in Appendix C are discussed in detail in the attached document. Internal Audit will conduct a follow-up audit to verify management's action plans have been implemented and are working as expected.

We appreciate the assistance and cooperation you and your staff provided during the performance of this audit. Please feel free to contact me at 980-314-2889 if you have any questions or concerns.

c: County Manager
Assistant County Managers
Deputy County Attorney
Senior County Attorney
Board of County Commissioners
Audit Review Committee

BACKGROUND

The information technology (IT) environment has evolved substantially over the past decade and mobile devices, such as smartphones and tablets, are now common ways for employees to connect to their organization's data and computing resources.

Mobile devices offer a range of convenience and productivity-enhancing features. These benefits come, however, with increased security risks. For example, their small size makes them easily lost or stolen; their weak user authentication mechanisms can be easily compromised or disabled by the user; and their constant connection to an organization's network allows more opportunity for unauthorized access. Accordingly, mobile devices have become one of the latest developments that must be properly managed throughout the asset's lifecycle to minimize the risk of sensitive or confidential information being exposed or stolen.

At a very basic level, asset lifecycle management is a set of business practices that integrates people, processes and technology to support strategic decision-making for the IT environment. Figure 1 below depicts the phases of a simplified asset lifecycle management process.

Figure 1: Asset Lifecycle Management

Mobile Device Management

Mecklenburg County's Technical Services Division within Information Technology Services (ITS) oversees the County's telecommunication services and mobile device distribution throughout the organization. The Asset and Facility Management Department (AFM) manages the County's warehouse operation where mobile devices ordered from vendors are initially received.

County departments use Cherwell, ITS' information technology service management system, to order mobile devices except for iPads and Surface Pros, which are ordered through Advantage, the County's financial management system.

The AFM warehouse staff initially receives and validates all mobile device shipments against the shipping and/or procurement documents. The AFM staff enters iPad and Surface Pro inventory data into Cherwell and WASP, AFM's inventory management system. Other mobile devices are not recorded in Cherwell and WASP. All mobile devices are transferred to ITS and WASP is updated.

The ITS staff deploys all mobile devices and updates iPad and smartphone user data in AirWatch, the ITS mobile device management system. AirWatch is updated when iPads and smartphones are retired.

COUNTY MANAGER'S OVERALL RESPONSE

The County Manager concurs with all action plans and implementation timeframes.

RISK OBSERVATIONS AND MITIGATION STRATEGIES

Risk Factor	Criticality	Design	Operation
1. Policies and Procedures Risk	🔴	🔴	🔴

Risk Observations

1.1 Department Formal Documentation (ITS)—Information Technology Services did not have documented, department-level policies and procedures for mobile device inventory management. Yet, policies and procedures are important control activities to help ensure management's directives are carried out while mitigating risks that may prevent the organization from achieving its objectives.

1.2 Department Formal Documentation (AFM)—While Asset and Facility Management had formal, documented policies and procedures for some aspects of its mobile device inventory management activities, they did not reflect some current and leading practices.

1.3 Enterprise Formal Documentation—Enterprise policies and procedures regarding mobile device management and utilization did not exist.

Recommendations

1.1 Internal Audit recommends ITS management develop and document formal policies and procedures for mobile device inventory management. Staff should be trained accordingly. The policies and procedures should be consistent with applicable County requirements, and include at a minimum:

- Essential operational activities, e.g., acquisition, purchase, storage, transfers, deployment, decommissioning, physical security, system access, physical inventory, segregation of duties, document retention, and management oversight
- Staff training requirements
- Staff roles and responsibilities
- Periodic procedure reviews and updates
- Internal and external communication requirements

1.2 Internal Audit recommends AFM management update its mobile device inventory management policies and procedures to incorporate relevant details regarding:

- Essential operational activities, e.g., inventory receipt and transfer, physical security, system access, physical inventory, segregation of duties, document retention, and management oversight
- Staff training

- Staff roles and responsibilities
- Policy and procedure reviews and updates
- Internal and external communication requirements

1.3 Internal Audit recommends ITS management, in collaboration with County departments, develop and document consistent and comprehensive policies and procedures for enterprise mobile device management and utilization. The policies and procedures should be consistent with applicable County requirements, and leading best practices, such as:

- Establishing ITS as the centralized authority over mobile device management and utilization processes and controls
- Developing department guidance for the mobile device lifecycle, including usage monitoring and inventory management.

Management's Response

1.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** October 2019

Action Plan: Develop a centralized IT asset management function responsible for lifecycle management, protection and controls of County software and technology equipment.

- Update existing policies and procedures for mobile device inventory management
- Update existing policies and procedures for mobile device utilization
- Post new policies and procedures on Meckweb for employee access

1.2 **Risk Mitigation Strategy:** Reduce **Implementation Date:** June 2018

Action Plan: Mobile device procedures have been developed and warehouse policies have been revised. Policies and procedures will be reviewed annually and revised when changes are required due to changing business needs. Management is implementing additional procedures to verify that operational activities are being performed as expected. All warehouse staff have been trained on warehouse policies and procedures, and any new staff will be trained upon arrival. Due to limited staffing all warehouse staff members have shared responsibilities.

1.3 **Risk Mitigation Strategy:** Reduce **Implementation Date:** October 2019

Action Plan: See ITS management's response at 1.1

Risk Factor	Criticality	Design	Operation
2. Existence Risk	🔴	🔴	🔴

Risk Observation

2.1 Asset Management—The ITS did not have a mobile device inventory. A critical security control for computing environments is an accurate and up-to-date inventory of technology assets.

Recommendation

2.1 Internal Audit recommends ITS management develop and maintain an inventory of all mobile devices. Moreover, ITS should implement processes and controls that utilize inventory and asset management best practices, such as:

- Perpetual inventory listings for all mobile devices
- Independent count, reconciliation, and verification
- Physical inventory discrepancy follow-up
- Segregation of duties

Management's Response

2.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** December 2019

Action Plan: Build an IT Asset Management function within ITS responsible for enterprise technology asset management and capture a comprehensive inventory of mobile devices.

Risk Factor	Criticality	Design	Operation
3. Physical Security Risk			

Risk Observation

3.1 Physical Access—While physical access to the AFM central warehouse and ITS mobile device storage locations was secured using keys, badges, etc., access was not always restricted to those with a valid business need. Failure to limit physical access increases the risk of loss or theft.

Recommendation

3.1 Internal Audit recommends AFM and ITS management limit physical access to the central warehouse and mobile device storage locations to only authorized staff with a business need. Further, management should periodically review physical access permissions. Last, management should retain documentation of their review.

Management's Response

3.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** November 2018

Action Plan: ITS management will limit access via badge authorization to specific staff. Additionally, ITS will store mobile device inventory in a locked storage room controlled by badge access to limited staff and review physical access controls at least annually with the understanding that terminated employees are already immediately removed from the network including access control databases.

3.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** June 2018

Action Plan: AFM management will review security access on a quarterly basis and retain documentation to verify this review.

Risk Factor	Criticality	Design	Operation
4. System Access Risk	🔴	🔴	🔴

Risk Observation

4.1 Logical Access—AirWatch and WASP system access was not limited to only staff with a valid business purpose. Further, ITS and AFM did not have a process to document justification for access, management approval, and type of access granted. As a result, AirWatch and WASP data may be vulnerable to loss or unauthorized modifications or disclosures.

Recommendation

4.1 Internal Audit recommends ITS and AFM management limit AirWatch and WASP system access to staff with a valid business need. We further recommend management formally approve, document, and periodically validate AirWatch and WASP system access rights. In addition, management should retain documentation of these control activities.

Management's Response

4.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** September 2018

Action Plan: ITS will limit AirWatch access to ITS staff with specific job responsibilities inside that system. In addition, IT Security will review employee access to AirWatch and make policy changes on a quarterly basis. If changes are required for access to AirWatch, a Cherwell ticket will be opened, documented and approved by IT Security. Quarterly reports will be maintained by IT Security to document control activities.

4.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** June 2018

Action Plan: AFM Management will review WASP access on a quarterly basis and retain documentation to verify this review.

Risk Factor	Criticality	Design	Operation
5. Segregation of Duties Risk	🔴	🟡	🟡

Risk Observation

5.1 Mobile Device Procurement—A single staff person both ordered and received all mobile devices, except for iPads and Surface Pros, and also reviewed the vendors' bills for appropriateness. Allowing a single individual to carry out incompatible duties within a process increases the risk of loss or theft.

Recommendation

5.1 Internal Audit recommends ITS management separate incompatible duties or implement appropriate compensating controls to mitigate the risks.

Management's Response

5.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** December 2018

Action Plan: ITS management will segregate duties of staff assigned to mobile device ordering, receiving and deployment.

Risk Factor	Criticality	Design	Operation
6. Compliance Risk	🔴	🟢	🟡

Risk Observation

6.1 Process Execution—Key tasks to manage smartphones, iPads, and Surface Pros were not consistently performed in alignment with management's directives. For example:

- Some smartphone devices were ordered without formal authorization documents
- Ordering and receiving documents were not always maintained to validate shipments were properly authorized and received
- Cherwell, AirWatch, and WASP system records did not always reflect ordering, receiving, and/or deployment activities to effectively manage mobile devices
- Mobile device custody records were not always retained to evidence accountability

Recommendation

6.1 Internal Audit recommends ITS management provide routine staff oversight of the mobile device lifecycle, i.e., acquisition, storage/management, deployment, and retirement/disposal. In addition, Internal Audit recommends AFM management provide staff oversight of mobile device receiving, storage/management, and transfer to ITS. Both ITS and AFM management should retain documentation of their reviews.

Management's Response

6.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** December 2018

Action Plan: ITS management will provide internal oversight (periodic validation) of device lifecycles with documentation of reviews. The quarterly reports will be maintained by ITS security personnel.

6.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** June 2018

Action Plan: In addition to quarterly physical inventory counts, AFM Management will perform random monthly audits of inventory received from receipt to transfer to ITS. This will be documented and retained. This will be adjusted to a quarterly basis when management feels the process is working well.

APPENDIX A—Risk Factor Definitions

Risk Factor	Definition
Accounting Risk	Failure to accurately and timely record transactions may result in untimely or inaccurate compilation of information needed for financial and operational reporting and analysis.
Compliance Risk	Failure to comply with established policies, procedures, and/or statutory requirements may result in unacceptable performance that impacts financial, operational, or customer objectives.
Existence Risk	Inadequate ability to track, monitor, and validate the existence of assets may result in the loss or diversion of such assets.
Human Resources Risk	Failure to attract, train, develop, deploy, and/or empower competent personnel may inhibit the organization's ability to execute, manage, and monitor key business activities.
Policies and Procedures Risk	Failure to formally document, clearly state, and update policies and procedures may result in poorly executed processes and/or increased operating costs.
Physical Security Risk	Inadequate physical security may allow unauthorized access to information system resources.
Segregation of Duties Risk	Failure to adequately segregate duties may allow an employee or group of employees to perpetrate and conceal errors or irregularities without timely detection.
System Access Risk	Failure to appropriately restrict access to information system resources may result in unauthorized access or changes to confidential information, and/or inefficiencies where access is too restrictive.

APPENDIX B—Color Code Definitions

The criticality of a risk factor represents the level of potential exposure to the organization and/or to the achievement of process-level objectives before consideration of any controls in place (inherent risk).

Criticality	Significance and Priority of Action
🔴	The inherent risk poses or could pose a significant level of exposure to the organization and/or to the achievement of process level objectives. Therefore, management should take immediate action to address risk observations related to this risk factor.
🟡	The inherent risk poses or could pose a moderate level of exposure to the organization and/or to the achievement of process level objectives. Therefore, management should take prompt action to address risk observations related to this risk factor.
🟢	The inherent risk poses or could pose a minimal level of exposure to the organization and/or to the achievement of process level objectives. Risk observations related to this risk factor, however, may provide opportunities to further reduce the risk to a more desirable level.

The assessment of the design and operation of key controls indicates Internal Audit's judgment of the process and system design to mitigate risks to an acceptable level.

Assessment	Design of Key Controls	Operation of Key Controls
🔴	The process and system design does not appear to be adequate to manage the risk to an acceptable level.	The operation of the process' risk management capabilities is not consistently effective to manage the risk to an acceptable level.
🟡	The process and system design appear to be adequate to manage the risk to an acceptable level. Failure to consistently perform key risk management activities may, however, result in some exposure even if other tasks are completed as designed.	The operation of the process' risk management capabilities is only partially sufficient to manage the risk to an acceptable level.
🟢	The process and system design appear to be adequate to manage the risk to an acceptable level.	The operation of the process' risk management capabilities appears to be sufficient to manage the risk to an acceptable level.

APPENDIX C—Risk Mitigation Strategy Definitions

Risk Mitigation Strategy	Definition
Reduce	Risk response where actions are taken to reduce a risk or its consequences.
Accept	Risk response where no action is taken to affect the risk.
Transfer	Risk response where a portion of the risk is transferred to other parties.
Avoid	Risk response to eliminate the risk by avoiding or withdrawing from the activity giving rise to the risk.