



**Mecklenburg County
Department of Internal Audit**

Business Support Services Agency
Computer and Equipment Disposal Audit
Report 1352

June 10, 2014

**Internal Audit's
Mission**

Through open communication, professionalism, expertise and trust, Internal Audit assists executive management and the Audit Review Committee in accomplishing the Board's objectives by bringing a systematic and disciplined approach to evaluate the effectiveness of the County's risk management, control and governance processes in the delivery of services.

**Internal Audit
Contacts**

Joanne Whitmore, CPA, CIA, CFE, CFF, CRMA, Audit Director
(704) 336-2575 or joanne.whitmore@mecklenburgcountync.gov

Christopher Waddell, CIA, CRMA, Audit Manager
(704) 336-2599 or christopher.waddell@mecklenburgcountync.gov

**Staff
Acknowledgements**

Richard Kring, CISA, Auditor-In-Charge

**Obtaining Copies of
Internal Audit Reports**

This report can be found in electronic format at
<http://charmeck.org/mecklenburg/county/audit/reports/pages/default.aspx>



MECKLENBURG COUNTY Department of Internal Audit

To: Brian Cox, Director, Business Support Services Agency
From: Joanne Whitmore, Director, Department of Internal Audit
Date: June 10, 2014
Subject: Computer and Equipment Disposal Audit Report 1352

The Department of Internal Audit has completed its audit of the Business Support Services Agency to determine whether internal controls over computer and equipment disposal effectively manage key business risks inherent to the activity. Internal Audit interviewed key personnel, evaluated policies and procedures and other documents, and tested various computer equipment and disposal activities from July 1, 2012 through June 30, 2013.

Internal Audit conducted this audit under the guidance of the 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 computer and equipment disposal were managed to an acceptable level; however, opportunities exist to improve the design and operation of some control activities.

The Business Support Services Agency—Information Technology (BSSA-IT) has already implemented physical security improvements for computers awaiting disposal to minimize access to computers that may contain confidential data.

RISK OBSERVATION SUMMARY

The table below summarizes the risk observations identified during the course of the 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 Formal Documentation			
2. Existence Risk	●	●	●
2.1 Reconciliations			
3. Data Destruction Risk	●	●	●
3.1 Hard Drive Sanitization			

The risk observations and management’s risk mitigation strategies are discussed in detail in the attached document. Internal Audit will conduct a follow-up review at a later date to verify management’s action plans have been implemented and are working as expected.

We appreciate the cooperation you and your staff provided during this audit. Please feel free to contact me at 704-336-2575 if you have any questions or concerns.

- c: County Manager
- Deputy County Manager
- Assistant County Managers
- Deputy County Attorney
- Senior County Attorney
- Board of County Commissioners
- Audit Review Committee
- Chief Technology Officer

BACKGROUND

The Business Support Services Agency—Information Technology (BSSA-IT) manages the County's information technology infrastructure, including data and voice networks, the Internet, servers, supporting application systems, computer replacement and disposal, and County data and systems security.

Computer and Equipment Disposal

The Business Support Services Agency—Asset and Facility Management (BSSA-AFM) manages the County's contract with a local vendor who provides computer, equipment, and furniture recycling. The vendor also destroys the hard drive storage devices of recycled computers by shredding the hard drives into metal strips. The BSSA-AFM receives the vendor's settlement documents, which lists the disposed computers and equipment.

The recycling vendor is ISO 14001, ISO 9001, and R2 certified¹, meeting ISO's international standards governing environmental and quality standard and recycling practices. The vendor's procedures also conform to the National Institute of Standards and Technology (NIST) Special Publication 800-88 Guidelines for Media Sanitation. Because County computers may have protected health information stored on the hard drives for computers waiting for recycling, the County needs to comply with the Health Insurance Portability and Accountability Act (HIPAA) requirements, which the vendor's certifications and procedures meet.

Multifunction printers, whose hard drives may also contain confidential data, are provided by a separate vendor. Their contract specifies machine hard drives must be erased prior to moving or replacing the devices.

Computer Replacement Program (CReP)

Mecklenburg County designates a percentage of each fiscal year's information technology budget for the Computer Replacement Program, which ensures County employees are provided computers that conform to a certain technology standard. The BSSA-IT determines what computers are replaced based on equipment age, warranty, work demands, and software requirements and then identifies what computer equipment is designated for disposal or redeployment.

¹ The ISO (International Organization for Standardization) is a developer of voluntary International Standards covering many aspects of technology and business.

COUNTY MANAGER'S OVERALL RESPONSE

The County Manager concurs with all risk mitigation strategies and timeframes for implementation.

RISK OBSERVATIONS AND MITIGATION STRATEGIES

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

Risk Observation

1.1 Formal Documentation—The existing Property Disposal and Redeployment policy and procedure no longer represents current responsibilities and processes at the County. In addition, management does not consistently conduct periodic policy and procedure reviews and updates. 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.

Recommendation

1.1 Internal Audit recommends management develop formal, documented policies and procedures for computer and equipment disposal activities that reflect current and best practices, and train staff as necessary. The policies and procedures should include, at a minimum:

- Staff roles and responsibilities for computer disposal activities
- Computer pre-disposal physical security
- Reconciliation between computer intake and destruction
- Hard drive sanitation methodology and timing
- Annual inventory requirements
- Policy application, including exceptions
- Periodic review and update of policies and procedures

Management's Risk Mitigation Strategy

1.1 Policies and procedures are presently being reviewed and amended to align computer and equipment disposal best practices with our business policies, processes and procedures. The aforementioned review and amendment process will be fully implemented by September 30, 2014. Benchmarked guidelines will be derived from NIST Special Publication-800-88.

a. Staff roles and responsibilities for computer disposal activities:

Action: Desktop technicians are responsible for exchanging in-service and decommissioned computers, destined either for repurpose or sanitization/destruction. A serial number, make and model for each unit are recorded by the technician in the Information Technology Services Management (ITSM) ticketing system to log the item. Subsequent to logging the information, the technician will deliver the computer to the BSSA-IT lab. When the computer physically arrives at the lab, the serial number, make and model of the device are entered into a logbook to verify that the computer has been accepted at the lab location.

If a computer/device is to be repurposed, the drive is reimaged for the new user, and a status change is logged in the ITSM system identifying the new owner. Before the computer/device physically leaves the BSSA-IT lab for redeployment, an exit entry is made to the lab log.

For computer/devices headed for disposal, documentation (Certificate of Sanitization) is created by a BSSA-IT technician. A copy of the Certificate of Sanitization is faxed to the recycle vendor requesting an equipment pickup. When the vendor arrives to claim the inventory, a review and verification of the decommissioned equipment is acknowledged by the vendor at the time of retrieval. The vendor will sign the Certificate of Sanitization acknowledging receipt of the decommissioned equipment. Once the vendor has physically destroyed the data drives, the vendor will send an itemized report of destroyed computer equipment to BSSA-AFM. BSSA-AFM will then forward a copy to the BSSA-IT desktop team to verify and validate a match of the original list faxed to the vendor. The information associated with this process will be entered into the ITSM to finalize the process.

b. Computer pre-disposal physical security:

Action: When a computer reaches “end of life” status or is remitted to BSSA-IT because an employee has been transitioned; each device will be evaluated to determine if it is going to be reused, or destroyed. The computer equipment will be tagged, logged, and secured until the final disposition has been determined. All equipment will be secured in a room or container with a locking mechanism, until such time as it is reused, or destroyed. Equipment disposition will be logged and maintained in an inventory database.

c. Reconciliation between computer intake and destruction

Action: In accordance with 1.1 subsection b (Computer pre-disposal physical security), a desktop technician will document the service tag number of the device, along with additional pertinent information specific to the item, in a destruction log. The log will reflect information contained in a “Certificate of Sanitization” record. A copy of the “Certificate of Sanitization” and a bill of lading will be provided to the county’s preferred recycling vendor. Upon destruction of the computer, the recycling vendor will provide to the BSSA-IT, on a quarterly basis, a reconciliation statement. The information contained in this statement will be substantiated, item by item, with BSSA-IT’s destruction log entries. BSSA-IT is already logging devices tagged for destruction. We will start the reconciliation process utilizing the vendors’ reports ending June 30, 2014.

d. Hard drive sanitation methodology and timing:

Action: After a determination has been made to either reuse or destroy the device, the hard drive of that device will either be reused or destroyed. Any device slated for reuse will have the hard drive(s) sanitized in accordance with Department of Defense (DOD) standard 5220.22-M.

Devices scheduled to be destroyed, will undergo hard drive(s) extraction and follow the process described in section 1.1 sub section b (Computer pre-disposal physical security). Computer information such as serial number, service tag number, hard drive identification numbers, and other information contained in the Certificate of Sanitization will be recorded in the destruction log. Drives set aside for destruction will then be physically destroyed via a hard drive destruction device to be purchased by BSSA-IT before April 15, 2014.

The desktop team will retain each hard drive for two weeks after its receipt from the employee. The data will serve as a back-up ensuring all migrated data has been transferred to the employee's new computer. The sanitation methodology will be in place June 30, 2014.

e. Annual inventory requirements:

Action: An inventory recordation policy and processes will be developed to ensure that a complete computer inventory is conducted on an annual basis. BSSA-IT is currently reviewing various methodologies that will allow for a complete and accurate inventory. This process will be finalized September 30, 2014.

f. Policy application, including exceptions:

Action: Quarterly reviews, by staff and management, will ensure that policies are being adhered to. Any deviation from the policies will be reviewed on a case by case basis, for example, a computer that is a litigation hold.

g. Periodic review and update of policies and procedures:

Action: An annual review of the policies will be conducted in the fourth quarter of each calendar year in accordance with an annual BSSA-IT leadership policy review.

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

Risk Observation

2.1 Reconciliations—The BSSA-IT does not perform reconciliation between the computers picked up by the vendor for destruction and the hard drives destroyed by the vendor. As a result, computers designated for destruction may not be properly decommissioned, exposing any confidential data contained on the hard drives to the risk of unauthorized disclosure.

Recommendation

2.1 Internal Audit recommends management reconcile computers slated for destruction against the vendor's settlement reports, which denotes computer hard drives that have been destroyed.

Management's Risk Mitigation Strategy

- 2.1 Reconciliation between disposal vendor and computer inventory list verifying decommissioning.
 Action: Please see response 1.1 sub-section c, this reconciliation will occur quarterly and exceptions will be reported to information security within one business day. Information security will then work with all interested parties to remediate the discrepancy and provide a detailed report to BSSA-IT senior leadership.

Risk Factor	Criticality	Design	Operation
3. Data Destruction Risk	●	●	●

Risk Observation

- 3.1 Hard Drive Sanitization—While the BSSA-IT sanitizes the hard drives for computers slated for redeployment to other County employees, computer hard drives in computers designated for destruction are not sanitized prior to vendor pick-up. As a result, confidential data that may be contained on the hard drives is not appropriately safeguarded against unauthorized disclosure.

Recommendation

- 3.1 Internal Audit recommends management implement procedures to sanitize hard drives in computers designated for destruction prior to vendor pick-up.

Management’s Risk Mitigation Strategy




- 3.1 Resolve: Hard drives designated for destruction are not sanitized prior to vendor pickup: Confidential data may be contained on hard drives. Moreover, the possibility of confidential data not being appropriately safeguarded against unauthorized disclosure is uncertain.
 Action: Please see response 1.1 sub-section d.

APPENDIX A—Risk Factor Definitions




Risk Factor	Definition
Policies and Procedures Risk	Policies and procedures that are non-existent, ineffective, unclear, or outdated may result in poorly executed processes and increased operating costs.
Data Destruction Risk	Failure to completely remove computer data and programs from redeployed and decommissioned computer equipment may result in unauthorized disclosure of restricted or confidential information.
Existence Risk	Inability to track, monitor, and validate the disposition of assets may result in loss or diversion of such assets.

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 <i>significant</i> 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 <i>moderate</i> 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 <i>minimal</i> 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 adequacy 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.