



**Mecklenburg County  
Department of Internal Audit**

Department of Financial Services  
Wire Transfers  
Report 2163

February 15, 2022

---

**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](mailto:joanne.prakapas@mecklenburgcountync.gov)

Crystal Turner, CIA, CFE, Audit Manager  
(980) 314-2894 or [crystal.turner@mecklenburgcountync.gov](mailto:crystal.turner@mecklenburgcountync.gov)

---

**Staff**

Rebecca Testin, CIA, CPA, Auditor-in-Charge

**Acknowledgements**

---

**Obtaining Copies of  
Internal Audit Reports**

This report can be found in electronic format at  
<https://www.mecknc.gov/audit/reports/pages/default.aspx>



**MECKLENBURG COUNTY**  
**Department of Internal Audit**

**To:** David Boyd, Director  
Department of Financial Services

**From:** Joanne Prakapas, Director  
Department of Internal Audit

**Date:** February 15, 2022

**Subject:** Department of Financial Services Wire Transfers Audit Report 2163

The Department of Internal Audit has completed its audit of the Department of Financial Services Wire Transfers 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 activities from July 1, 2019 through April 30, 2021.

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 the wire transfers process were managed to an acceptable level; however, opportunities exist to improve the design and operation of some control activities.

## RISK OBSERVATION SUMMARY

The table below summarizes the risk observations identified during 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 Departmental Formal Documentation			
1.2 Enterprise Formal Documentation			
1.3 Periodic Review			
2. System Access Risk	●	●	●
2.1 User Recertification			
3. Accounting Risk	●	●	●
No risk observations noted			
4. Communication Risk	●	●	●
No risk observations noted			
5. Compliance Risk	●	●	●
No risk observations noted			
6. Human Resources Risk	●	●	●
No risk observations noted			
7. Fraud Risk	●	●	●
No risk observations noted			
8. Segregation of Duties Risk	●	●	●
No risk observations noted			

<b>RISK OBSERVATION SUMMARY (con't.)</b>			
<b>Risk Factors and Observations</b>	<b>Criticality</b>	<b>Design</b>	<b>Operation</b>
9. Payment Accuracy Risk	●	●	●
No risk observations noted			
10. Receipt Risk	●	●	●
No risk observations noted			

The risk observations and management’s risk mitigation strategies defined in Appendix C are discussed in detail in the attached document. Internal Audit will conduct a follow-up review 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
- Deputy County Managers
- County Attorney
- Deputy County Attorney
- Board of County Commissioners
- Audit Review Committee

## BACKGROUND

The Department of Financial Services is responsible for the administration of County finances in accordance with State laws and budget ordinances established by the Mecklenburg Board of County Commissioners. These administrative activities include but are not limited to investments of County money; financial reporting; cash flow and banking debt management; budgetary compliance; payroll; and accounts payable.

There are three divisions—Central Finance, Departmental Financial Services (DFS), and Procurement, in which Central Finance is primarily responsible for wire transfer activities.

### Wire Transfers

A wire transfer is an electronic transfer of money, allowing large, time-sensitive funds to make same-day payment transfers to or from the County’s operating accounts. Sending or receiving large dollar payments electronically reduces the risk of large checks being lost, stolen, or delayed in the mail.

### Outgoing Wire Transfers

The most common outgoing wire transfers are payments to cities and townships for their portion of collected taxes, and well as employee benefit payments, e.g., retirement and health benefits.

To ensure outgoing wire transfers are properly authorized, there are two levels of approvals by Central Finance before the transfer can be processed. Both approvals must be made to process a wire transfer for payment. The investment officer is the first approver, reviewing the request and supporting documentation, verifying the information, and entering the wire transfer into the County’s banking system. A secondary approver then authorizes and submits the wire transfer to the vendor’s bank account.

Outgoing Wire Transfers		
Fiscal Year	Number of Wire Transfers	Dollar Amount
2019	1,041	\$ 1,213,394,004
2020	999	1,207,911,367
2021	934	1,213,061,470
<b>Total</b>	<b>2,974</b>	<b>\$ 3,634,366,841</b>

*Source: Advantage Financial System, unaudited*

### Incoming Wire Transfers

The most common incoming wire transfers are tax payment receipts, federal, and State grants. The Office of the Tax Collector (OTC) receives incoming wire transfers for property tax payments and debt set-off payments (delinquent taxes). The OTC records the payment information into the North Carolina Property Tax System (NCPTS), the State's tax system that supports the collection of property taxes. Incoming wires for Public Health, Social Services, and Criminal Justice Services are transferred into the County's bank account. Central Finance staff records the payments in Advantage, the County's accounting system.

Incoming Wire Transfers		
Fiscal Year	Number of Wire Transfers	Dollar Amount
2019	182	\$ 635,561,988
2020	165	726,687,786
2021	159	700,294,487
<b>Total</b>	<b>506</b>	<b>\$ 2,062,544,261</b>

*Source: Advantage Financial System, unaudited*

### Investment Wire Transfers

The investment officer monitors the County's cash flow and prepares a daily cash and investment activity report that includes investment interest; investment purchases and withdrawals; incoming and outgoing wire transfers; and other cash flow activities. Investment related wire transfers are initiated by the investment officer and approved in the daily cash process. The Director of Finance approves the daily cash and investment activity report.

### Reconciliation Process

Central Finance staff monthly reconciles incoming and outgoing wire activities to the bank statements, ensuring all incoming and outgoing wires have been captured and properly recorded in Advantage. Central Finance staff prepares the monthly bank reconciliation, and an independent person reviews and approves any necessary adjusting journal entries.

## 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 Observations

- 1.1 Department-level Documentation—While Central Finance had formal, documented Standard Operating Procedures (SOP) for outgoing wire transfers, they did not have SOPs to guide staff on processing incoming wire transfers. Yet, procedures are important control activities to help management ensure its directives are carried out while mitigating risk that may prevent the organization from achieving its objectives.
- 1.2 Enterprise-level Documentation—While the enterprise-level Cash Handling, Receipts, and Deposit policy existed for some aspects of wire transfer activities, it did not reflect current practices, e.g., staff roles and responsibilities.
- 1.3 Review and Approval—While Central Finance developed a formal process to routinely review, update, and approve both department- and enterprise-level financial policies and procedures, they had not reviewed the County’s Cash Handling, Receipts and Deposits policy since October 2018, which is not compliant with department policy.

### Recommendations

- 1.1 Internal Audit recommends management develop department-level SOPs for incoming wire transfers and communicate the procedures to County departments. Procedures should include, at a minimum:
  - Essential operational activities, e.g., incoming wire request, documentation, management approvals, and management oversight
  - Staff roles and responsibilities
  - Training requirements
- 1.2 Internal Audit recommends management update its enterprise-wide Cash Handling, Receipts, and Deposit policy specific to electronic payments, which includes wire transfers, to reflect current staff roles and responsibilities.
- 1.3 Internal Audit recommends management ensure its policies and procedures are routinely reviewed, updated, and approved according to department policy. The review should be documented, and staff should be trained accordingly.

**Management’s Response**

1.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** January 2022

**Action Plan:** The existing Wire Request and Processing Policy will be updated to incorporate departmental-level SOPs for incoming wires and communicated to County departments.

1.2 **Risk Mitigation Strategy:** Reduce **Implementation Date:** January 2022

**Action Plan:** The Cash Handling, Receipts, and Deposit policy will be updated; however, policies and procedures associated with incoming wires will be incorporated into the Wire Request and Processing Policy as described in recommendation response 1.1.

1.3 **Risk Mitigation Strategy:** Reduce **Implementation Date:** January 2022

**Action Plan:** All Finance policies will be regularly reviewed, updated as necessary, and approved according to department policy. The review will be documented, and staff trained accordingly.

Risk Factor	Criticality	Design	Operation
2. System Access Risk	●	●	●

**Risk Observation**

2.1 User Recertifications—A terminated employee had banking and investment system access rights to perform account inquiries, run client reports, transfer assets, purchase, and redeem investments for at least three months after termination. Bank and investment user access privileges were not reviewed on a periodic basis to ensure the level of privileges remained appropriate. In addition, employee status changes are not timely communicated to system administrators. The lack of a periodic provisioning and reprovisioning increases the risk that excessive or inappropriate access privileges will not be timely detected or removed.

**Recommendation**

2.1 Internal Audit recommends management formally approve, document, and periodically validate banking and investment system account privileges. Management should document their review and notify the appropriate system administrators of any changes made to employees’ access in the banking and investment systems.

**Management’s Response**

2.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** January 2022

**Action Plan:** Banking and investment system privileges will routinely be approved and reviewed. Management’s review will be documented, and appropriate system administrators notified of any changes made to employees’ access in the banking and investment systems.

**APPENDIX A—Risk Factor Definitions**

<b>Risk Factor</b>	<b>Definition</b>
Accounting Risk	Failure to accurately and timely record transactions may result in untimely or inaccurate compilation and reporting of information needed for financial analysis, external reporting of financial results or internal analysis of operating results.
Communication Risk	Failure to foster consistent and effective communication may result in misunderstandings regarding service delivery and/or customer expectations.
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.
Fraud Risk	Failure of employees, vendors, or other parties to carry out their activities in compliance with the law and ethical standards of the organization may result in fraud.
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.
Payment Accuracy Risk	Inadequate execution of outgoing wire processes may result in payments to vendors for the incorrect amount or duplicate payments. Inadequate review of outgoing transfers may result in errors or omissions in accounting information.
Policies and Procedures Risk	Failure to have formal, documented, clearly stated, and updated policies and procedures may result in poorly executed processes and/or increased operating costs.
Receipt Risk	Failure to properly receipt incoming wire transfers may result in untimely or inaccurate compilation and reporting information needed for financial or internal analysis of operating results.
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 do 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 designs 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 designs 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**

<b>Risk Mitigation Strategy</b>	<b>Definition</b>
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.