



Audit and Ethics Committee Meeting

Sep 23, 2026 8:00 AM - 8:30 AM CDT

NES Board Room 121

-
1. Safety Moment - Daniel Johnson
 2. Recommendation for approval of minutes of the Audit and Ethics Committee meeting held August 26, 2026
 3. Recommendation for approval of the Annual Auditor's Report and Financial Statements - Tabitha Beach
 4. Internal Audit Reports - Baker Tilly - Scott Nalley
 - 4.1. Audit and Ethics Committee Calendar
 - 4.2. Internal Audit Status Report
 - 4.3. FY27 Audit Plan Revisions
 - 4.3.1. Recommendation for approval
 - 4.4. Internal Audit Report - Storm Expenditures
 - 4.5. Internal Audit Report - Meter to Cash
 - 4.6. Recommendations - Meter to Cash
 - 4.7. Internal Audit Report - Network and Cybersecurity Corporate
 - 4.8. Recommendations - Network and Cybersecurity Corporate
 - 4.9. Internal Audit Report - Purchased Power
 - 4.10. Q4 FY26 Follow-Up and Remediation
 5. Executive Session
 6. Miscellaneous

Emergency Preparedness: Be Ready Before the Emergency

September is Emergency Preparedness Month, a reminder that the best time to prepare for an emergency is before it occurs.

At NES, preparedness is a year-round commitment. Whether responding to severe weather, equipment failures, cyber incidents, or other emergencies, our ability to protect employees, serve customers, and restore service efficiently depends on the work we do before an event takes place.

Preparedness begins with understanding our roles, maintaining clear lines of communication, ensuring resources are available, and being ready to make sound decisions under challenging circumstances. The same principle applies to our customers. Simple steps such as maintaining an emergency kit, knowing how to report an outage, having safe backup power options, and establishing a family communication plan can significantly improve resilience during an emergency.

The objective is straightforward: prepare before the event, respond safely during the event, and recover as quickly as possible afterward. Safety does not begin when an emergency starts. It begins with preparation.

AUDIT AND ETHICS COMMITTEE MEETING MINUTES AUGUST 26, 2026

The Audit and Ethics Committee meeting was held on Wednesday, August 26, 2026.

Committee Members Present: Clifton Harris, Casey Santos, Jaz Boon, and Ian Prunty

Officers Present: Teresa Broyles-Aplin, Laura Smith, Dr. Trish Holliday, Brad Heck, and Tabitha Beach

Acting Chair Casey Santos called the meeting to order at 8:11 a.m.

OATH OF OFFICE

Assistant Secretary Dr. Trish Holliday administered the Oath of Office for NES's new board member, Robert D. 'Jaz' Boon II, and requested that he recite the Oath of Office for the record. His five-year term of office commenced on July 21, 2026, and expires on July 1, 2031.

SAFETY MOMENT

Vaughan Charles presented a safety moment on newly licensed drivers.

MINUTES

Upon motion by Member Harris and seconded by Member Prunty, the Committee approved the minutes from the Audit and Ethics Committee meeting held July 22, 2026, with four ayes and zero nays.

EVALUATION OF INTERNAL AUDIT SURVEY RESULTS

Ms. Santos reported that in accordance with the Committee's oversight responsibilities and the Institute of Internal Auditors standards, the Committee conducted its annual assessment of the effectiveness of the Internal Audit function. To support this review, all Committee members completed an Internal Audit evaluation survey.

Overall, the Committee expressed a high level of satisfaction with the performance of the Internal Audit function and concluded that its activities remain aligned with the organization's strategic objectives and governance framework.

The Committee will continue to monitor the Internal Audit function through its regular oversight responsibilities and annual evaluation process to support sustained effectiveness, accountability, and alignment with professional standards.

BAKER TILLY INTERNAL AUDIT REPORT

Scott Nalley reviewed the Audit and Ethics Committee Calendar and Internal Audit Status Report and provided an update on Baker Tilly's audit of the Physical Security and Employee Safety

processes. He stated that the audit identified no high-risk issues within the scope reviewed and noted the related findings.

Mr. Nalley noted that three audits from the FY26 audit plan remain to be presented, and it is expected that those will be ready for the September Audit and Ethics Committee meeting.

Chair Santos referenced the audit's review of emergency response procedures and asked if the proper procedures were being utilized. Mr. Nalley indicated that no issues were found within the scope of the audit.

PRICEWATERHOUSECOOPERS FISCAL YEAR 2026 AUDIT RESULTS

Chris Lorenz presented PricewaterhouseCoopers' Fiscal Year 2026 audit results. He stated that there were no significant changes to the audit plan presented on April 22, 2026, and that final materiality thresholds remained consistent with preliminary planning thresholds.

Mr. Lorenz reported that PricewaterhouseCoopers had substantially completed the audits of the financial statements and expected to issue its unqualified opinions in September 2026. He noted that a draft of the audit reports could be found in Appendix II.

He stated that no matters had been identified related to independence or other required communications that would reasonably be expected to impact independence. He also confirmed that no material or known fraud had been identified. Mr. Lorenz added that there were no identified instances of non-compliance with laws or regulations, unrecorded misstatements, or matters that rose to the level of a material weakness.

Member Prunty asked for more information regarding oversight in the AI era. Mr. Lorenz responded that the rapid evolution of AI is empowering companies to solve problems in unprecedented ways. He noted that its transformative potential also creates new avenues for growth, innovation, and strategic business development. He stated that this power does not come without risks. Realizing the full potential of AI requires understanding its risks as well as its benefits. This includes a risk management approach and appropriate policies, processes, and controls to use AI responsibly in a manner that sustains trust.

MISCELLANEOUS

There were no miscellaneous items to present.

EXECUTIVE SESSION

There was no Executive Session held.

ADJOURNMENT

The meeting adjourned at 8:27 a.m.

APPROVED: _____
Acting Committee Chair Casey Santos

**RECOMMENDATION FOR APPROVAL OF
THE ANNUAL AUDITORS' REPORT AND FINANCIAL STATEMENTS**

PwC has completed its examination of the financial statements of Nashville Electric Service for fiscal year ending June 30, 2026. The firm presented their audit report and all other required communications to the Audit Committee last month.

The Board has adopted a program for voluntary compliance with certain provisions of the Sarbanes-Oxley Act. One of the adopted provisions is that the Audit and Ethics Committee will review and approve the annual financial statements. Copies of the financial statements have been circulated to all members of the Committee.

Management recommends approval of the financial statements and the referenced reports.

Internal Audit Reports – Baker Tilly

**THE ELECTRIC POWER BOARD
OF THE METROPOLITAN GOVERNMENT
OF NASHVILLE AND DAVIDSON COUNTY**

AUDIT & ETHICS COMMITTEE CALENDAR

COMMITTEE ACTIONS	1st Qtr*	2nd Qtr*	3rd Qtr*	4th Qtr*	As Needed
EXTERNAL AUDITORS					
Advise the Board as to appointment and compensation of the external audit firm					X
Review external audit plan		April			
Confirm independence of external auditors		April	August		X
Review any “second opinions” obtained on accounting and financial reporting policies					X
Receive external communications required under generally accepted auditing standards		April	August		
Review and consider completeness of financial statements and consistency of information with that known and make recommendation to the Board as to approval			August		
Review management letter (e.g., control deficiencies)			August		
Review status of management letter corrective actions			August		
Review performance of external auditors and make recommendation to Board regarding appointment or discharge					X
EXECUTIVE MANAGEMENT					
Consider the effectiveness of internal controls	X	X	X	X	
Review Enterprise Risk Management program				November	
Review letter of representations certifying appropriateness of financial statements and disclosures			August		
INTERNAL AUDIT					
Approve the Internal Audit Charter			July		X
Advise the Board as to appointment and compensation of the internal audit firm			July		X
Review and approve the annual audit plan			July		
Review and approve changes to the audit plan			July		X
Review effectiveness of internal audit function			July		X
Review compliance with IIA standards			July		X
Confirm organizational independence			July		

COMMITTEE ACTIONS	1st Qtr*	2nd Qtr*	3rd Qtr*	4th Qtr*	As Needed
COMPLIANCE					
Review effectiveness of system for monitoring compliance	X	X	X	X	
Review findings of examinations of regulatory agencies					X
OTHER					
Receive board training	X				
Review the process for monitoring conflicts of interest				October	
Evaluate committee calendar					X
Evaluate committee performance				X	

* Calendar year

**Nashville Electric Service
Internal Audit Status Report
As of September 23, 2026**

CURRENT AUDITS	
Audit Description	Date Started
Capital Projects and Capitalization Process	August 2026
Corporate Governance and Legal	September 2026
Infrastructure Design and Construction	September 2026
UPCOMING AUDITS	
Audit Description	Scheduled Start Date
Q1 FY27 Follow-Up and Remediation	October 2026
Travel Expenses	November 2026
Property, Plant, and Equipment	January 2027
Board, Executive, and Employee Accounts	January 2027
Q2 FY27 Follow-Up and Remediation	January 2027
Timekeeping and Payroll	March 2027
Vegetation Management Lifecycle	March 2027
Cybersecurity Operations	April 2027
Q3 FY27 Follow-Up and Remediation	April 2027
Information Technology (IT) Department Controls	May 2027
Emergency Response Plan and Outage Reporting	May 2027
Meter Reading and Meter Maintenance	May 2027
NON-AUDIT SERVICES	
Service Description	Status/Scheduled Date
Enterprise Risk Management Assistance	In-Process
ServiceNow Integrated Risk Management (IRM) Assistance	Complete
Fraud Risk Assessment	In-Process
Oracle Time and Labor Implementation Project	In-Process
Completed AUDITS	
Audit Description	Completion Date
Physical Security and Employee Safety (FY26)	August 2026
Storm Expenditures (FY26)	September 2026
Meter to Cash (FY26)	September 2026
Network and Cybersecurity - Corporate (FY26)	September 2026
Purchased Power	September 2026
Q4 FY26 Follow-Up and Remediation	September 2026

To: Audit Committee of the NES Electric Power Board
From: Scott Nalley, Director Internal Audit
Subject: Approval of Revised FY27 Internal Audit Plan
Date: September 23, 2026

The internal audit Standards require Internal Audit to maintain a dynamic, risk-responsive audit plan and communicate changes to the audit plan to the Audit Committee.

Internal Control Framework (ICF) Refresh - At the request of NES management, Internal Audit will assist management in refreshing NES' existing Internal Control Framework (ICF), which was originally developed based on the COSO 2013 Internal Control-Integrated Framework to document management's system of internal control over financial reporting in an effort to aid management in their compliance with T.C.A. 9-18-102 (Financial Integrity Act). The need for the ICF refresh is primarily due to system implementations and upgrades, such as C2M/WAM, and Ellipse which support underlying transactions that impact the general ledger and financial reporting, as well as recent organizational realignments that impact responsibilities and ownership of internal controls.

We expect our participation in this project to occur during the months of October and November 2026, and to take approximately 200-250 hours. We propose increasing the approved FY27 budget line item "Internal Control Framework Assistance" by 250 hours to accommodate this project.

Oracle Time and Labor System Implementation - At the request of NES management, Internal Audit will assist management in identifying considerations of system design, testing and functional use of the Oracle Time and Labor application. Internal Audit will provide independent project consulting during the system configuration and implementation. The Oracle Time and Labor application will replace PeopleSoft, which is NES' current time and labor reporting tool.

We expect our participation in this project to occur during the period August 2026 through January 2027 and to take approximately 125 hours. This project is an addition to the FY27 audit plan.

Internal Audit has evaluated staffing and co-sourcing capacity and confirms that the revised plan is achievable with current resources.

Request for Audit Committee Approval

We are requesting Audit Committee approval of the proposed revisions to the FY27 Internal Audit Plan. The original FY27 Internal Audit Plan included total budgeted hours of 6,990 and with the proposed additions the revised FY27 Plan budgeted hours are 7,365. **(Appendix A).**

Appendix A

Nashville Electric Service Revised Audit Plan - Fiscal Year 2027

Audit Description	Audit Type	Hours
Cybersecurity Operations	Integrated	350
Board, Executive, and Employee Accounts	Operational	115
Travel Expenses	Operational	100
Information Technology (IT) Department Controls	IT	500
Capital Projects and Capitalization Process	Integrated	450
Timekeeping and Payroll	Integrated	600
Infrastructure Design, Construction, and Capitalization	Integrated	500
Corporate Governance and Legal	Integrated	600
Emergency Response Plan and Outage Reporting	Integrated	450
Meter Reading and Meter Maintenance	Integrated	550
Property, Plant, and Equipment	Integrated	400
Vegetation Management Lifecycle	Integrated	600
Purchased Power and TVA Programs	Integrated	375
Additional Items		
Planning, Administration, and Consulting		350
Internal/External Quality Assurance and Improvement Program		100
Audit Committee and Board Meetings		100
Risk Assessment		75
<i>Internal Control Framework (ICF) Assistance/ICF Refresh</i>		<i>400</i>
ERM Assistance		375
Follow-up and Remediation-Quarterly		250
<i>Oracle Time and Labor System Implementation</i>		<i>125</i>
Total FY27 Audit Plan Hours		7,365
Total FY26 Audit Plan Hours (excluding additional project hours)		7,200
Total FY25 Audit Plan Hours (excluding additional project hours)		7,040
Total FY24 Audit Plan Hours (excluding additional project hours)		6,740

Recommendation for Approval of the Revised FY27 Internal Audit Plan.

Internal Audit recommends approval of the revised FY27 Internal Audit Plan which includes 7,365 hours.



Nashville Electric Service

FY2026 Storm Expenditure Review

Internal Audit Report

For the Period: January 23, 2026 through March 31, 2026



CONFIDENTIAL

This report is intended solely for the use of management and the Board of Directors and should not be used for any other purpose. The Company's external auditors may be provided with a copy of this report in connection with fulfilling their responsibilities.

Nashville Electric Service

Storm Expenditure Review Internal Audit – FY2026

Table of Contents

I. Executive Summary	2
II. Overview of Results	3
III. Findings and Conclusion Summary	4
IV. Findings and Recommendations	6

Report Distribution:	<u>Name</u>	<u>Title</u>
	Tabitha Beach	Interim CFO
	Trish Holliday	VP Chief People Officer
	Matt Dodd	Interim Corporate Controller
	Sandra Chapman	Controls & Compliance Manager

Additional Distribution:	<u>Name</u>	<u>Title</u>
	Rob McCabe	Audit Committee Chair
	Teresa Broyles-Aplin	President & CEO
	Laura Smith	Interim EVP & Chief Legal Officer
	Brad Heck	Interim COO
	Ron Womble	CIO

I. Executive Summary

Introduction

Baker Tilly Advisory Group, LP has performed certain internal audit services for Nashville Electric Service (NES) related to the **Storm Expenditure** process. Our fieldwork was performed April 15, 2026 through June 30, 2026. The audit covered the period from January 23, 2026 through March 31, 2026. Our primary objective was to independently and objectively test and assess the internal controls related to **Storm Expenditures**. Our services were performed in accordance with the terms of our contract with an effective date beginning on June 1, 2026. We conducted this audit in accordance with the *Global Internal Audit Standards issued by the Institute of Internal Auditors*. 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.

Background

Winter Storm Fern was a weather event that impacted NES' service territory in late January 2026, bringing ice and prolonged freezing temperatures that caused widespread system outages. This was the largest outage event in NES history. At the peak of the event, the storm impacted nearly 50% of NES' customers and required 12 days to reach full restoration. NES incurred approximately \$103 million in storm related costs associated with emergency response and restoration activities. As a municipal utility, certain storm related costs may be eligible for reimbursement through the Federal Emergency Management Agency's (FEMA) Public Assistance Program. NES is responsible for identifying, accumulating, and maintaining appropriate documentation to support eligible costs submitted to FEMA for reimbursement.

Internal audit, NES management, and the Audit & Ethics Committee agreed that the significant financial cost warranted the need for an internal audit dedicated to storm related expenses.

Scope

We evaluated the design and operating effectiveness of key controls. Areas of audit emphasis included, but were not limited to, determining whether:

- Contracts are in place for all third-party contractors, including FEMA Mutual Aid contractors,
- Emergency processes (e.g., vendor selection and expedited onboarding, contract approval) implemented prior to and/or during the storm were appropriately documented and approved,
- Procurement and materials management processes were performed in accordance with policies and procedures and/or approved exceptions,

- Labor and overtime hours and rates were complete, accurate, and approved in accordance with policies and procedures and/or approved exceptions,
- Meal, hotel and travel costs were complete, accurate, and approved in accordance with policies and procedures and/or approved exceptions, and
- Vendor invoices, including materials and contract labor, were complete, accurate, billed at the agreed upon contracted rates, and approved in accordance with policies and procedures and/or approved exceptions.

As part of management's post-storm continuous improvement efforts, including recommendations resulting from an independent after-action assessment, management is implementing several initiatives to strengthen storm response processes. A key initiative includes developing and documenting storm-specific job duties and responsibilities for all employees based on the organization's five-tier storm severity classification, which should further enhance operational practices and the efficiency and effectiveness in capturing various storm related costs. Remediation efforts performed subsequent to the storm event were not considered in the scope of the audit.

Corporate Governance, Culture and Stewardship Considerations

We considered corporate governance, culture, and stewardship initiatives that may have an impact on the scope of the audit. We did not identify any extraordinary initiatives that had an impact on the audit scope. Inherently, many of the procedures performed in our audit are focused on governance activities.

II. Overview of Results

During the course of our work, we discussed potential findings with management. A summary of these findings is provided in **Section III** along with a summary and definition of our assessment of the risk level.

In order to enhance your understanding of each specific finding, we have provided a response priority, defined as follows:

High - Requires immediate management attention. This is a serious internal control or risk management issue that may, with a high degree of certainty, lead to substantial losses, serious reputational damage, or significant adverse impact.

Medium - Requires timely management attention. This is an internal control or risk management issue that may lead to financial losses, reputational damage, or adverse impact, such as public sanctions or immaterial fines.

Low - Routine management attention is warranted. This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the process being tested. Risks are limited.

Based on our procedures and assessment of the findings noted, we have provided an overall audit grade. The audit grade is not intended to usurp ultimate risk assessment responsibility, which is vested with the Audit Committee and management.

Overall audit grades are defined as follows:

Satisfactory - Findings are limited to minor deviations from policy or regulatory requirements resulting in nominal risk to NES. The design and operating effectiveness of controls evaluated during the audit appear adequate and reasonable. However, because of inherent limitations in any system of internal control, errors or irregularities may occur and not be detected. Therefore, absolute reliance should not be placed on these controls.

Needs Improvement - Findings include an aggregation of minor deviations and/or major deviations from policy or regulatory requirements resulting in reasonable probability of further misstatements or violations, if not corrected promptly. The design and operating effectiveness of controls evaluated during the audit appear to be less than adequate, and limited reliance can be placed on these controls.

Unsatisfactory - Findings include an aggregation of minor deviations and/or major deviations from policy or regulatory requirements resulting in probable misstatements or violations that could be significantly detrimental to NES. Immediate corrective action by high-level management, the Audit Committee, and possibly the Board will be desirable. Findings in this category will immediately be reported to the appropriate level to ensure timely action can be taken. The design and operating effectiveness of controls evaluated during the audit are not effective and should not be considered reliable.

III. Findings and Conclusion Summary

Based on the scope of the audit, the following table portrays the number of audit findings by response priority. Red reflects audit findings that are considered high response priority, yellow reflects audit findings of medium response priority, and green reflects findings of low response priority.

Internal Audit Area	Auditor's Grade	High	Medium	Low	Page
Storm Expenditures:					
Labor Tracking	Satisfactory	-	1	-	6
Meal Provisioning		-	1	-	7
Overtime Reporting		-	1	-	8
Total		-	3	-	

Conclusion Summary

There were no high risk issues identified during our procedures. The findings noted do not appear to represent a significant risk at this time. However, our recommendations to these findings provide an opportunity for NES to strengthen internal controls. Our detailed findings and recommendations are described in **Section IV** of this report.

We appreciate the cooperation extended to us by personnel at NES and are pleased to be of service. If there are any questions or comments regarding this report, please contact us. Contact information for the Director and Assistant Director of Internal Audit responsible for this work is presented below.

Scott Nalley, CIA, CISA, CISSP
Director of Internal Audit
615-782-4252
Scott.Nalley@bakertilly.com

Patrick Clark, CIA
Assistant Director of Internal Audit
615-921-5997
Patrick.Clark@bakertilly.com

IV. Findings and Recommendations

Finding 2026-01: Labor Tracking

Response Priority: **Medium**

Controls over the documentation of storm related job duties are not sufficient to ensure that all eligible storm work, including storm related administrative activities performed by supervisory personnel and above, is consistently captured and recorded timely. During testing of labor hours charged to the storm work order, we identified the following:

- At least 4 managers in Operations potentially performed administrative activities eligible for FEMA reimbursement who did not have time reported to the storm work order or on a FEMA management cost tracking worksheet.
- Eleven of 45 employee time reports tested did not have documented and approved description of job duties performed during the storm as of June 24, 2026, 135 days after the storm work order closed on February 9, 2026. Additionally, some job duty descriptions appeared to be generic and may be inadequate to support the hours charged. FEMA reporting requires a description of job duties performed to be included for all internal labor submissions. As of July 2026, job duty descriptions for all employees have been obtained and provided to the FEMA coordinator (Controls and Compliance Manager).

Risk: Incomplete support for labor costs incurred increases the risk of delayed reimbursement submissions, delayed reimbursement, or disallowed labor costs, or otherwise limits the ability to identify and recover all eligible FEMA reimbursement costs.

Recommendation:

1. Human Resources management should lead an effort to implement an Operational Playbook to outline requirements for capturing storm related administrative and management costs to replace the current manual process. The solution should enable employees to record hours worked, select FEMA-eligible work activities, and capture supporting information in a standardized format that improves data quality, reporting consistency, and reimbursement readiness.
2. Accounting management should communicate to Supervisors and above the FEMA guidelines for eligible administrative time and reporting requirements as well as the expectations and responsibilities based on roles to help ensure all eligible time is captured and reported to NES' FEMA coordinator.

Management's Response:

1. Management recognizes that storm related duties, including administrative and coordination performed by supervisors and senior personnel, must be captured with enough detail to demonstrate the relationship between the labor cost and eligible storm work. All field superintendents and managers have not consistently reported in the system of record hours that exceed their regularly scheduled work hours because these positions are FLSA exempt and are also ineligible for overtime compensation within NES Policy. As we continue to operationalize the Four Pillars initiative, the expectations, procedures, and communication requirements for reporting hours and allocating to work orders for these roles will be defined within the applicable NES Storm/Event Operational Playbook.
2. Storm roles are being developed under the Incident Command System process. Management will establish a process that captures roles and responsibilities of the storm process and communicate documentation expectations for future events.

Responsibility: Trish Holliday and Tabitha Beach

Implementation Date:

1. June 30, 2027
2. December 31, 2026

Finding 2026-02: Meal Provisioning

Response Priority: **Medium**

Controls over the administration and documentation of storm related meal benefits are not standardized across the organization to ensure employees receive only one meal benefit for the same overtime work period, either a catered meal or an overtime meal allowance (processed through payroll). Participation in catered meals was not consistently documented at the individual employee level across the organization. As a result, sufficient information is not available for us or management to perform a reconciliation to confirm that only one meal benefit was provided. During our review, we tested to determine if employees attending a catered meal also claimed a meal allowance on a sample basis using the available information and did not identify instances where an employee received both a catered meal and meal allowance benefit. However, during review of overtime meal allowances across all locations, we determined that there was no notable difference in the number of overtime meal allowances claimed on days when catered meals were not available as on days when catered meals were available.

Risk: The absence of standardized processes and supporting documentation for catered meal participation increases the risk of duplicate meal benefits, incorrect FEMA reimbursement submissions, and a lack of cost control.

Recommendation: Human Resources management should establish and implement a standardized process across all operating locations for administering and documenting storm related meal benefits. At a minimum, the process should require documentation of individual employee participation in catered meals through attendance rosters, badge scans, electronic sign-in, or another verifiable method. In addition, management should consider performing spot checks or an overall analysis to compare employees who received catered meals with employees who claimed overtime meal allowances through the timekeeping and payroll systems. Any discrepancies or possible duplicate meal benefits should be investigated and resolved.

Management's Response: Documentation and subsequent review processes will be implemented as a standard for the organization when a meal is catered by NES during an emergency event. This process will be included in the applicable NES Storm/Event Operational Playbook.

Responsibility: Trish Holliday

Implementation Date: June 30, 2027

Finding 2026-03: Overtime Reporting

Response Priority: **Medium**

Storm related overtime policies do not include pre-defined storm related job duties at the employee level, which makes it difficult to assess the business need for overtime recorded, and to determine if overtime is accurately and appropriately reported (over or under). During testing of overtime hours charged to the storm work order, we determined that although overtime was approved through the established timekeeping and approval processes, the storm related work descriptions provided did not always clearly demonstrate the necessity of overtime, particularly for non-operations employees. In several instances, overtime reporting varied among employees performing similar functions, making it difficult to assess the appropriateness and consistency of overtime reporting during the storm event.

Risk: The lack of clearly defined storm related job duties and adequate supporting documentation increases the risk that overtime hours may be inaccurately reported, inconsistently charged, or not sufficiently supported to validate the appropriateness and necessity of the overtime incurred.

Recommendation: Human Resources management, in collaboration with executive leadership, should establish pre-defined storm-specific job responsibilities and work expectations based on storm severity levels and expected duration to provide a stronger basis for validating overtime worked, improve consistency of overtime reporting, and establish a pre-defined basis for when storm related overtime may be necessary. Additionally, management should recommunicate department specific storm related overtime policies to employees and supervisors, including documentation requirements and provide additional training, if needed, to ensure all employees are aware of the policies and supervisors and managers know how to apply and enforce them with consistency during a storm event.

Management's Response: The implementation of a formal Incident Command System includes all employees having a predetermined storm role, responsibility, and expectation. Employees in roles that typically do not work overtime, or emergency assignments may be expected to maintain a summary of work performed to substantiate total recorded hours. This process will be included in the applicable NES Storm/Event Operational Playbook.

Responsibility: Trish Holliday

Implementation Date: June 30, 2027



Nashville Electric Service

FY2026 Meter to Cash

Internal Audit Report

For the Period: May 1, 2025 through April 30, 2026



CONFIDENTIAL

This report is intended solely for the use of management and the Board of Directors and should not be used for any other purpose. The Company's external auditors may be provided with a copy of this report in connection with fulfilling their responsibilities.

Nashville Electric Service

Meter to Cash
Internal Audit – FY2026

Table of Contents

I. Executive Summary	2
II. Overview of Results	3
III. Findings and Conclusion Summary	5
IV. Findings and Recommendations	6

Report Distribution:	<u>Name</u>	<u>Title</u>
	Aleisha Johnson	Interim VP Customer Relations
	Tabitha Beach	Interim CFO
	Barry Daniel	Revenue and Rates Manager
	Sonya Pullens	Customer Relations Manager
	Suzanne Hamilton	Interim Customer Solutions Sr. Manager
	Vaughan Charles	VP Grid Transformation & Project Mgt.
	Tony Richman	Engineering Manager
	Carla Nelson	Engineering Supervisor

Additional Distribution:	<u>Name</u>	<u>Title</u>
	Rob McCabe	Audit Committee Chair
	Teresa Broyles-Aplin	President & CEO
	Laura Smith	Interim EVP & Chief Legal Officer
	Brad Heck	Interim COO
	Trish Holliday	VP Chief People Officer
	Ron Womble	CIO

I. Executive Summary

Introduction

Baker Tilly Advisory Group, LP has performed certain internal audit services for Nashville Electric Service (NES) related to the customer setup, security deposit management, meter read processing, billing, and payment collection processes. Our fieldwork was performed June 2026 through July 2026. The audit covered the period from May 1, 2025 through April 30, 2026. Our primary objective was to independently and objectively test and assess the internal controls related to **Meter to Cash**. Our services were performed in accordance with the terms of our contract with an effective date beginning on June 1, 2026. We conducted this audit in accordance with the *Global Internal Audit Standards issued by the Institute of Internal Auditors*. 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.

Scope

During the period covered by the audit, Customer to Meter (C2M) post-implementation procedures were in place and the organization experienced a significant storm event in early 2026. During the course of the audit, we considered the impacts of these two circumstances, including exceptions to standard processes such as a revised disconnect/reconnect process, waiving late fees, extended payment arrangements, and managing high volumes of estimated bills. We evaluated the design and operating effectiveness of key controls. Areas of audit emphasis included, but were not limited to, determining whether:

- Policies and procedures related to customer setup, security deposits, meter reading, billing, credit and collections, and payment collections are established, and kept current,
- Customer accounts, service agreements, customer classes, rate codes, and billing determinants are established and maintained accurately within C2M,
- Customer deposits are collected and refunded in accordance with NES policy, as applicable,
- Meter reads and usage data transmitted from metering and third-party systems into C2M are complete, accurate, and processed timely,
- Meter read validation, editing, estimation, and exception handling are operating effectively to ensure billing accuracy,
- To-Do workflows in C2M are routed and monitored effectively to ensure timely resolution of exceptions,
- Customers are billed in accordance with applicable rate classes, including both energy and customer charges approved by TVA and the NES Power Board,
- Estimated bills are generated accurately and in accordance with internal policies,
- Sales tax is billed and collected from customers, as applicable by law,

- Other fees (e.g., late fees, meter test fees, AMI opt-out fees) are billed, in accordance with NES policy,
- Adjustments to customer accounts are authorized and properly supported in accordance with NES policy,
- Customer billing information transferred to third party vendors is complete and accurate, and properly secured in accordance with NES policy,
- Customer payments are collected, processed, and posted accurately and timely to the appropriate customer accounts within C2M,
- Payment arrangements are approved, calculated, and monitored, in accordance with internal policies,
- Disconnections and reconnections are initiated and billed accurately and in accordance with internal policies,
- Interfaces between C2M and third-party payment processors, banking institutions, and other integrated systems are complete, accurate, and properly monitored,
- Outstanding customer account balances are monitored, written off, and sent to collections, in accordance with NES policy, and
- User access to C2M, ePortal (customer account manager and paperless billing provider), Doxim (bill print provider), Paymentus (electronic bill presentment and payment service provider), and DebtNext (debt management software) is properly restricted according to assigned roles and responsibilities.

Corporate Governance, Culture and Stewardship Considerations

We considered corporate governance, culture, and stewardship initiatives that may have an impact on the scope of the audit. Internal Audit met with Revenue and Rates, Meter Services, and Customer Relations management and discussed governance, culture and stewardship considerations for the FY26 Meter to Cash audit. During these discussions, we determined that several programs are in place to assist customers with bill payment assistance, such as NeedLink and NES has other voluntary community/customer involvement programs such as Power of Change and Round-Up, whose funds are also used to support customer energy efficiency. We did not include a detailed review of these programs in the audit, but reviewed and validated related transactions such as payments, credits, and adjustments to customer invoices as these transactions may arise within our sample selections for testing various controls. Inherently, many of the procedures performed in our audit are focused on governance activities.

II. Overview of Results

During the course of our work, we discussed potential findings with management. A summary of these findings is provided in **Section III** along with a summary and definition of our assessment of the risk level.

In order to enhance your understanding of each specific finding, we have provided a response priority, defined as follows:

High - Requires immediate management attention. This is a serious internal control or risk management issue that may, with a high degree of certainty, lead to substantial losses, serious reputational damage, or significant adverse impact.

Medium - Requires timely management attention. This is an internal control or risk management issue that may lead to financial losses, reputational damage, or adverse impact, such as public sanctions or immaterial fines.

Low - Routine management attention is warranted. This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the process being tested. Risks are limited.

Based on our procedures and assessment of the findings noted, we have provided an overall audit grade. The audit grade is not intended to usurp ultimate risk assessment responsibility, which is vested with the Audit Committee and management.

Overall audit grades are defined as follows:

Satisfactory - Findings are limited to minor deviations from policy or regulatory requirements resulting in nominal risk to NES. The design and operating effectiveness of controls evaluated during the audit appear adequate and reasonable. However, because of inherent limitations in any system of internal control, errors or irregularities may occur and not be detected. Therefore, absolute reliance should not be placed on these controls.

Needs Improvement - Findings include an aggregation of minor deviations and/or major deviations from policy or regulatory requirements resulting in reasonable probability of further misstatements or violations, if not corrected promptly. The design and operating effectiveness of controls evaluated during the audit appear to be less than adequate, and limited reliance can be placed on these controls.

Unsatisfactory - Findings include an aggregation of minor deviations and/or major deviations from policy or regulatory requirements resulting in probable misstatements or violations that could be significantly detrimental to NES. Immediate corrective action by high-level management, the Audit Committee, and possibly the Board will be desirable. Findings in this category will immediately be reported to the appropriate level to ensure timely action can be taken. The design and operating effectiveness of controls evaluated during the audit are not effective and should not be considered reliable.

III. Findings and Conclusion Summary

Based on the scope of the audit, the following table portrays the number of audit findings by response priority. Red reflects audit findings that are considered high response priority, yellow reflects audit findings of medium response priority, and green reflects findings of low response priority.

Internal Audit Area	Auditor's Grade	High	Medium	Low	Page
Meter to Cash:					
Commercial Deposit Calculator	Satisfactory	-	1	-	6
Open Field Activities in C2M		-	1	-	7
Total		-	2	-	

Conclusion Summary

There were no high-risk issues identified during our procedures. The findings noted do not appear to represent a significant risk at this time. However, our recommendations to these findings provide an opportunity for NES to strengthen internal controls. Our detailed findings and recommendations are described in **Section IV** of this report.

We appreciate the cooperation extended to us by personnel at NES and are pleased to be of service. If there are any questions or comments regarding this report, please contact us. Contact information for the Director and Assistant Director of Internal Audit responsible for this work is presented below.

Scott Nalley, CIA, CISA, CISSP
Director of Internal Audit
615-782-4252
Scott.Nalley@bakertilly.com

Patrick Clark, CIA
Assistant Director of Internal Audit
615-921-5997
Patrick.Clark@bakertilly.com

IV. Findings and Recommendations

Finding 2026-01: Commercial Deposit Calculator

Response Priority: Medium

Controls have not been established to ensure the accuracy and ongoing maintenance of the manually maintained Excel-based commercial deposit calculator and its underlying rates and assumptions. During our testing, we determined that rates used in the Excel-based deposit calculator are not current, ownership has not been formally established, and a defined review and change-management process has not been established. As a result, the spreadsheet used to calculate deposits for new commercial customers may not consistently reflect current approved rates and business requirements. We were unable to calculate what the required deposits would have been using current rates, as the historical assumptions (e.g. business type, estimated square footage) used in the calculation are not retained, and therefore we are unable to determine the materiality or financial impact had the current rates been used. Assumptions entered in the spreadsheet are overwritten with each use. Customer Relations uses the manually maintained Excel-based calculator to estimate the required deposit for new commercial customers that do not have sufficient billing history. For commercial customers that do have sufficient billing history, C2M is configured to systematically calculate the required deposit. NES requires commercial customers to provide a security deposit or other acceptable form of financial assurance before service begins. The deposit is intended to mitigate NES' financial exposure in the event a customer does not satisfy future payment obligations. Commercial customers may satisfy or avoid the cash deposit requirement through other approved forms of financial assurance, including an Irrevocable Letter of Credit, Indemnity Bond, acceptable payment history with another gas or electric utility, or evidence of adequate financial credentials.

Risk: Security deposits for new commercial customers may be calculated using inaccurate or outdated rates and assumptions, resulting in deposits that are higher or lower than intended. This may lead to inconsistent application of deposit requirements, customer dissatisfaction, additional manual corrections, and financial exposure if deposits are insufficient to mitigate the intended credit risk.

Recommendation: Customer Relations management, in coordination with Engineering management, should establish controls over the commercial deposit calculation process. At a minimum, management should:

1. Assign clear ownership and accountability for maintaining the commercial deposit calculator and its underlying rates and assumptions, and

2. Establish and document procedures requiring rates and calculation assumptions to be reviewed, updated, tested, and approved following applicable rate changes or modifications to business rules.

Customer Relations management should also assess whether it is feasible to modify and implement an automated process within C2M to replace the current Excel-based spreadsheet and should consider retaining historical assumptions used in the Excel-based calculator to provide an audit trail.

Management's Response: The commercial deposit calculator is an exception process used only when sufficient prior billing history is not available in C2M to systematically calculate the required commercial deposit. When sufficient billing history is available, C2M is used to calculate the deposit.

Energy Services Engineering (ESE) will assume ownership of the commercial deposit calculator, including responsibility for maintaining the calculator and the rates, calculation methodology, and underlying assumptions used to determine commercial deposits.

ESE will provide Customer Relations with an updated, tested, and approved commercial deposit calculator annually following the October TVA rate change and whenever applicable rates, calculation assumptions, or business rules change. ESE will establish and document the process for reviewing, updating, testing, and approving the calculator prior to providing it to Customer Relations for use.

Customer Relations management will ensure the current deposit calculator is available to employees when determining deposits for applicable new commercial customers.

Responsibility: Aleisha Johnson, Sonya Pullens, and Carla Nelson

Implementation Date: October 1, 2026

Finding 2026-02: Open Field Activities in C2M

Response Priority: **Medium**

Field Activities may not be consistently monitored across the organization, and actual statuses may not be current in C2M. During our review, we identified a significant number of open Field Activities, including activities that have remained open for extended periods dating back to March 2025.

Field Activities are one of the core operational mechanisms that bridge customer service, billing, and the physical work performed in the field. A Field Activity is a structured work request generated within C2M that instructs field personnel to perform specific tasks such as new construction

activities, meter installations, meter exchanges and other service and maintenance activities at a service point/location. Field Activities may be generated automatically by C2M or created and assigned by various departments, including Customer Relations, Meter Services, and the Center of Excellence.

As of August 5, 2026, C2M contained 12,188 open Field Activities and are aged as follows:

Aging	Number of Open Field Activities
360 days or more	4,015
180 to 359 days	2,295
30 to 179 days	3,700
Less than 30 days	2,178
Total	12,188

We selected a sample of Field Activities created prior to 2026 which included various types such as; frequent outages, limb on wire, private light changes and vegetation management requests, and determined that for some Field Activities no recent activity within the past eight to twelve months was documented in C2M. Additionally, for some Field Activities created prior to April 1, 2025 no new activity was recorded in C2M since they were created. This may indicate that these Field Activities have not been worked, are no longer needed, or have been completed, but are not closed in C2M. Additionally, it may indicate that there is not a primary owner, or an established review process is not in place. Field Activity types have different expected completion timelines based on the nature and complexity of the work and some activities may appropriately remain open for extended periods, while others may warrant further review.

Risk: Field Activities that remain open beyond expected completion timeframes may result in inaccurate or outdated operational reporting, limiting management’s ability to effectively assess workload, resource utilization, service performance, and operational backlogs. Inadequate monitoring of aged activities also increases the risk that completed or cancelled work remains open or legitimate outstanding work is not followed up timely, potentially resulting in service delays, customer dissatisfaction, and reputational damage.

Recommendation: Customer Relations management should collaborate with the Center of Excellence and business operations managers to:

1. Review all open Field Activities and update statuses to their current state, which may include cancelling, closing, reassigning, etc., and
2. Establish and implement a process to periodically monitor and resolve aging Field Activities across all departments, taking into consideration the type of activity and its expected

lifecycle (i.e., expected duration to complete the activity) including defining ownership and escalation procedures.

Management's Response: Field Activities represent a broad range of work across multiple business groups, and the expected lifecycle varies significantly based on the type and complexity of the work. Therefore, the age of a Field Activity alone does not necessarily indicate that the activity is overdue or no longer being managed.

The Center of Excellence (CoE) will work with the applicable business groups to reconcile existing open Field Activities. As part of this effort, Field Activity types will be aligned with the appropriate business owner, and reasonable expected lifecycles will be established based on the nature of each activity type. Business owners will review activities that fall outside the established lifecycle and update, close, cancel, or otherwise resolve the activity as appropriate.

The CoE will also expand reporting available to business units to support ongoing monitoring of open and aging Field Activities. A regular review cadence will be established to provide business owners with visibility into activities that exceed the expected lifecycle for their respective activity types and support appropriate follow-up and resolution.

Responsibility: Aleisha Johnson and Suzanne Hamilton

Implementation Date: October 1, 2026



Nashville Electric Service Meter to Cash Recommendations and Best Practices

To: Tabitha Beach, Interim CFO, Barry Daniel, Revenue and Rates Manager, Aleisha Johnson, Interim VP Customer Relations, and Sonya Pullens, Customer Relations Manager

From: Baker Tilly

Date: August 27, 2026

During our review covering the period May 1, 2025 through April 30, 2026, the following areas were not considered to be findings within the audit report, but were noted as areas for potential improvement or are recommendations based on best practice:

ePortal User

One NES internal business user was identified as having inappropriate access to the ePortal application. ePortal is a customer self-service application that enables customers to manage their accounts online, including bill payments and requesting service reconnections. The user was appropriately granted access to the application in November 2022 based on their job responsibilities at that time. However, the individual transferred to another department in April 2025, at which point access to ePortal was no longer required to perform their assigned duties. Once identified by Internal Audit, the user's access was removed. Customer Relations management should continue to exercise due care when performing the annual user access review, with particular attention given to employees who have transferred departments or changed roles since the previous review to help ensure access remains appropriate for current job responsibilities.

Rate Sheet for Monthly Invoicing

The current rate sheet for NES' bill print service provider was not on file at the time of our review. Management was notified of an annual rate increase in January 2026, but did not obtain the approved rate sheet until June 2026, once identified by Internal Audit. Revenue and Rates management should obtain an updated rate sheet at the time they are notified of rate changes. Additionally, management should request that the provider's invoice be addressed to the current Revenue and Rates Manager, as invoices are currently addressed to the former Customer Relations manager who has retired.



Nashville Electric Service

FY2026 Network and Cybersecurity Corporate

Internal Audit Report
For the Period: June 1, 2025 through May 31, 2026



CONFIDENTIAL

*This report is intended solely for the use of management and the Board of Directors and should not be used for any other purpose.
The Company's external auditors may be provided with a copy of this report in connection with fulfilling their responsibilities.*

Nashville Electric Service

Network and Cybersecurity Corporate
Internal Audit – FY2026

Table of Contents

I. Executive Summary	2
II. Overview of Results.....	3
III. Findings and Conclusion Summary	4
IV. Findings and Recommendations	6

Report Distribution:	<u>Name</u>	<u>Title</u>
	Ron Womble	CIO
	Brent Catoe	IT Security Manager
	Troy Craig	IT Systems Manager

Additional Distribution:	<u>Name</u>	<u>Title</u>
	Rob McCabe	Audit Committee Chair
	Teresa Broyles-Aplin	President & CEO
	Laura Smith	Interim EVP & Chief Legal Officer
	Tabith Beach	Interim CFO
	Brad Heck	Interim COO

I. Executive Summary

Introduction

Baker Tilly Advisory Group, LP has performed certain internal audit services for Nashville Electric Service (NES) related to Network and Cybersecurity Corporate processes. Our fieldwork was performed from June 2026 through July 2026. The audit covered the period from June 1, 2025 through May 31, 2026. Our primary objective was to independently and objectively test and assess the internal controls related to **Network and Cybersecurity Corporate**. Our services were performed in accordance with the terms of our contract with an effective date beginning on June 1, 2026. We conducted this audit in accordance with the *Global Internal Audit Standards issued by the Institute of Internal Auditors*. 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.

Scope

We evaluated the design and operating effectiveness of key controls. Areas of audit emphasis included, but were not limited to, determining whether:

- Information Technology (IT) policies and procedures are in place, current, and approved,
- A defined IT Strategy is in place, including a plan to address current and future technology needs,
- Artificial Intelligence (AI) governance policies are established, and use of AI technologies comply with NES policy and best practices,
- Network access onboarding, removal, and certification is performed in accordance with NES policy,
- The identity and access management application is appropriately designed and configured to support management approvals and assignment of role-based access based on least privileged in accordance with NES policy,
- The network domain is adequately protected from outside threats, inside threats, human error, or harm from intentional or unintentional actions of staff,
- Endpoint applications are appropriately designed and configured to protect programs and data from loss, damage and unauthorized use,
- iPad devices are issued, tracked and maintained in accordance with NES Policy,
- Key network hardware and infrastructure are operating on supported and current operating systems,
- Changes to network infrastructure, including logical access, operating systems, and security device parameters, are authorized and documented in accordance with NES policy,

- Changes to key network systems are logged, tested, approved, and implemented in accordance with NES Policy,
- Unplanned or emergency application changes are authorized, documented and approved in accordance with NES Policy,
- Critical batch jobs and real time interfaces are monitored, and identified errors are addressed timely in accordance with NES policy,
- Backups of data and applications are performed, monitored, and identified errors are addressed timely, and off premise backups are maintained in accordance with NES Policy and best practices, and
- IT governance and oversight controls are in place and operating effectively.

Corporate Governance, Culture and Stewardship Considerations

We considered corporate governance, culture, and stewardship initiatives that may have an impact on the scope of the audit. We did not identify any extraordinary initiatives that had an impact on the audit scope. Inherently, many of the procedures performed in our audit are focused on governance activities.

II. Overview of Results

During the course of our work, we discussed potential findings with management. A summary of these findings is provided in **Section III** along with a summary and definition of our assessment of the risk level.

In order to enhance your understanding of each specific finding, we have provided a response priority, defined as follows:

High - Requires immediate management attention. This is a serious internal control or risk management issue that may, with a high degree of certainty, lead to substantial losses, serious reputational damage, or significant adverse impact.

Medium - Requires timely management attention. This is an internal control or risk management issue that may lead to financial losses, reputational damage, or adverse impact, such as public sanctions or immaterial fines.

Low - Routine management attention is warranted. This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the process being tested. Risks are limited.

Based on our procedures and assessment of the findings noted, we have provided an overall audit grade. The audit grade is not intended to usurp ultimate risk assessment responsibility, which is vested with the Audit Committee and management.

Overall audit grades are defined as follows:

Satisfactory - Findings are limited to minor deviations from policy or regulatory requirements resulting in nominal risk to NES. The design and operating effectiveness of controls evaluated during the audit appear adequate and reasonable. However, because of inherent limitations in any system of internal control, errors or irregularities may occur and not be detected. Therefore, absolute reliance should not be placed on these controls.

Needs Improvement - Findings include an aggregation of minor deviations and/or major deviations from policy or regulatory requirements resulting in reasonable probability of further misstatements or violations, if not corrected promptly. The design and operating effectiveness of controls evaluated during the audit appear to be less than adequate, and limited reliance can be placed on these controls.

Unsatisfactory - Findings include an aggregation of minor deviations and/or major deviations from policy or regulatory requirements resulting in probable misstatements or violations that could be significantly detrimental to NES. Immediate corrective action by high-level management, the Audit Committee, and possibly the Board will be desirable. Findings in this category will immediately be reported to the appropriate level to ensure timely action can be taken. The design and operating effectiveness of controls evaluated during the audit are not effective and should not be considered reliable.

III. Findings and Conclusion Summary

Based on the scope of the audit, the following table portrays the number of audit findings by response priority. Red reflects audit findings that are considered high response priority, yellow reflects audit findings of medium response priority, and green reflects findings of low response priority.

Internal Audit Area	Auditor's Grade	High	Medium	Low	Page
Network and Cybersecurity Corporate:					
iPad Device Management	Satisfactory	-	1	-	6
Unnecessary System Access		-	-	1	7
Incomplete Demand Ticket Supporting Documentation		-	-	1	8
Excessive Access to Firewall Tickets		-	-	1	9
Total		-	1	3	

Conclusion Summary

There were no high risk issues identified during our procedures. The findings noted do not appear to represent a significant risk at this time. However, our recommendations to these findings provide an opportunity for NES to strengthen internal controls. Our detailed findings and recommendations are described in **Section IV** of this report.

We appreciate the cooperation extended to us by personnel at NES and are pleased to be of service. If there are any questions or comments regarding this report, please contact us. Contact information for the Director and Assistant Director of Internal Audit responsible for this work is presented below.

Scott Nalley, CIA, CISA, CISSP
Director of Internal Audit
615-782-4252
Scott.Nalley@bakertilly.com

Patrick Clark, CIA
Assistant Director of Internal Audit
615-921-5997
Patrick.Clark@bakertilly.com

IV. Findings and Recommendations

Finding 2026-01: iPad Device Management

Response Priority: Medium

iPad device deployment and ongoing support does not align with NES policy nor best practices. Prior to Winter Storm Fern, NES was in the process of rolling out iPad devices to select business groups. As a result of the storm, the rollout of iPads was expedited to allow NES employees to more easily support storm and vegetation crews. During our testing of iPads, we identified the following, which appeared to be related to the expedited rollout during Winter Storm Fern:

- Four of nine devices sampled were not on the latest operating system security patch,
- One of nine devices sampled could not be examined to determine if the device was patched because the device had never been set-up. It is our understanding that upon set-up, the user could avoid installing current patches. Per the employee, the device was not set-up due to lack of employee training. Given that the device remains unused, the device may not be necessary for the employee's job responsibilities,
- 37 were not correctly assigned in ManageEngine. Thirty-six of these devices were assigned to two employees to support storm work and their device assignment record was not updated upon completion of the work and return of the devices.

Risk: Insufficient device patching, assignment records, and employee training increases the risk that iPads are not appropriately secured, tracked, or available for their intended business purpose. Unpatched devices may expose systems to known security vulnerabilities, while inaccurate device assignments may limit the ability to maintain accountability of company assets. Insufficient training can result in unintended waste of resources if assigned devices are not used.

Recommendation: IT management should enhance processes around iPad device management. In addition, IT management should evaluate whether their patch management system can appropriately address the needs of the iPad patching program, update assignment records when iPads are returned, and periodically provide employee training around iPad usage to ensure users know how to utilize issued devices.

Management's Response: IT management will review and modify existing patching processes to ensure all NES issued mobile devices are patched in accordance with IT standards. Additionally, processes will be created to ensure that iPad ownership is updated as employees move within or leave the organization. IT will review and modify training processes for new iPad deployments to ensure basic device training requirements are met.

Responsibility: Ron Womble, Troy Craig

Implementation Date: January 31, 2027

Finding 2026-02: Unnecessary System Access

Response Priority: Low

Access to critical business systems is not always reviewed timely or based on least privilege. Over the past year, NES implemented two critical systems (Oracle C2M and WAM) and made significant updates to the Ellipse application. The implementation and upgrade of these applications were supported by numerous contractors. During our review of direct access to these applications, we identified the following:

- Three accounts related to the implementation of C2M and WAM were not removed after go-live as access was no longer needed. Two of these accounts had superuser access to C2M and WAM. Upon discovery of the three accounts, access was removed, and
- Four accounts with direct access to Ellipse had not recently been used (two accounts since 2024 and two accounts since 2006). One of these accounts had system administrator access.

All of these accounts were at the application level and could not be used by non-IT employees.

Risk: Inadequate review and timely removal of unnecessary system access increases the risk that privileged or administrative accounts remain active after the business need for such access has ended. Unnecessary accounts with privileged access could be used to make unauthorized changes to critical systems or data, potentially resulting in data integrity issues, security incidents, or disruption to business operations. Additionally, failure to consistently perform user access reviews of direct access may limit management's ability to prevent or detect unauthorized activity within critical business systems.

Recommendation: IT management should implement processes to ensure that periodic reviews of direct access to critical production systems are performed in accordance with their risk-based review standard.

Management's Response: IT management will enhance existing access review processes to require annual recertification of all local (direct) access to critical NES systems, with approval of the system owner and product owner.

Responsibility: Ron Womble and Brent Catoe

Implementation Date: November 30, 2026

Finding 2026-03: Incomplete Demand Ticket Supporting Documentation

Response Priority: Low

Required steps for anticipated IT service needs (“Demands”) in ServiceNow are not always completed before being moved to the next step of the Demand process. Demands allow IT management to identify, organize, and plan for future business IT needs. During the past year, NES has been implementing Demand management following the Information Technology Infrastructure Library (ITIL) framework. As such, many of the Demand management processes were implemented during the audit scope period. During our testing of Demands, we identified the following:

- Business cases were not completed for four of 14 Demands sampled, prior to being moved to the submitted state, as required in the NES Demand Management Guide,
- Security reviews were not completed for two of 14 Demands sampled prior to Demand approval or being moved to the qualified state, as required in the NES Demand Management Guide,
- Architecture reviews were not completed for two of 14 Demands sampled prior to Demand approval or being moved to the qualified state, as required in the NES Demand Management Guide, and
- An approver did not appear to be documented for two of 14 completed Demands, as required in the Demand Management Guide.

Risk: Incomplete Demand support documentation could increase the risk that IT initiatives are approved without adequate consideration of business value, security risks, technical requirements, and alignment with company objectives. Additionally, Demands reviewed in an incomplete state may result in inefficiency, resulting in wasted time obtaining missing information. Missing approvals may limit management’s ability to demonstrate appropriate oversight and accountability for the investment of IT resources.

Recommendation: IT management should enhance training for the NES Demand Management Guide to ensure that users entering Demands in ServiceNow understand company processes.

Management’s Response: IT has implemented ServiceNow decision records to document Security and Architecture reviews and approvals, establishing a single system of records for demand governance decisions.

The IT PMO and Information Security will meet to conduct recurring reviews to track pending security assessments, ensure decisions are rendered, and verify documentation is recorded on associated demand records. Demand review meetings with Demand Managers will continue to monitor compliance with business case, approval, and documentation requirements. In addition, the IT Governance team will provide refresher training to Demand Managers on Demand Management Guide requirements, documentation standards, and role expectations.

Responsibility: Ron Womble and Kathleen Schwaber

Implementation Date: October 31, 2026

Finding 2026-04: Excessive Access to Firewall Tickets

Response Priority: Low

Access to ServiceNow firewall change tickets, which may include sensitive data, are not adequately restricted to authorized parties. During testing of firewall changes, we determined that 176 users, including third party support providers and NES employees not in IT, had access to firewall change tickets through their ServiceNow ITIL license. Third party support individuals and non-IT employees generally do not need access to firewall tickets, as they include sensitive configuration data such as ports and IP addresses.

Risk: Unnecessary access to firewall change tickets increases the risk that sensitive network configuration information, including IP addresses and port information, may be disclosed to individuals without a business need. Access to this information could provide insight into NES' network architecture and security controls used to secure the company network.

Recommendation: IT management should limit access to firewall change tickets to users with an appropriate business need.

Management's Response: IT is in the process of implementing a new system for Firewall Auditing, Reporting, and Change Requests. This new system will be independent of Service Now and will have Role Based Access Controls to ensure users only see firewall rules and firewall change requests relevant to systems that they support.

Responsibility: Ron Womble and Brent Catoe

Implementation Date: November 30, 2026



Nashville Electric Service Network and Cybersecurity Corporate Recommendations and Best Practices

To: Ron Womble, Brent Catoe, Troy Craig

From: Baker Tilly

Date: August 28, 2026

During our review covering the period June 1, 2025 through May 31, 2026, the following areas were not considered to be findings within the audit report, but were noted as areas for potential improvement or are recommendations based on best practice:

Best Practice Recommendations

- A comprehensive listing of all third-party Software-as-a-Service (SaaS) applications supporting NES operations does not currently appear to be maintained. While applications authenticating through the access management application are tracked, third-party applications that do not use this authentication method may not be captured. During testing, three known third-party applications were not included on the system-generated listing. Management indicated that the listing is currently being updated as part of the Disaster Recovery plan. Information Security management should develop a list of third-party applications which do not authenticate via their access management application to ensure that security practices can be audited and enforced throughout their control environment.
- ITIL licenses are not always used. During inspection of ITL licenses, eight users with access to ServiceNow had not logged in during the past 6 months, and three users had never logged in. IT Management should periodically review ServiceNow usage to determine if these licenses are needed.
- The IT Network Diagram has not been updated since July 2023 and does not currently reflect infrastructure changes from the removal of property and the addition of new systems since that time. Maintaining current network documentation is important to support proper IT Governance. IT Management should periodically review the IT Network Diagram to ensure it reflects the current IT Network.
- The approval process for new Generative AI tools is not consistent between the NES Policy Manual and the IT Gen AI Security Standard. The Policy Manual requires the functional vice president or designee to submit requests to IT, while the Security Standard allows individuals or departments to request approval from IT. The NES Policy Manual supersedes the Security Standard. IT management should consider aligning the IT Gen AI Security Standard with the NES Policy Manual to provide consistent and clear expectations regarding the process and authority for requesting approval of new Gen AI tools.
- Okta user access certification campaigns, which is the built-in user access review feature in Okta, are not consistently completed in their entirety. Information Security personnel indicated that incomplete campaigns could result from assigned certifiers not responding to Information Security inquiries, including reviewers in management positions. IT management should consider evaluating methods to improve

completion of access certification campaigns, which may include coordinating with Human Resources or other appropriate stakeholders to reinforce reviewer responsibilities and establish an escalation process for outstanding certifications.

- All requestable job roles within Okta do not have an assigned approver. During testing, 35 of 145 roles inspected did not have an assigned approver. When an approver is not assigned, access is not automatically granted and a manual research process is required before the request can proceed. IT management should consider periodically reviewing requestable Okta roles to ensure that all requestable roles have an assigned approver.
 - The Corporate Password Standard available on the NES SharePoint site does not reflect the current version of the standard. During testing, the posted document did not include changes to NES password requirements made in May 2025. Upon investigation by IT management, it was confirmed that the updated Corporate Password Standard was never posted. IT management should update the NES SharePoint site with the current Corporate Password Standard and consider establishing a process to help ensure that future revisions to IT standards are timely communicated and posted to the SharePoint site.
 - The Project Management Standard requires IT Security personnel to review projects at project formation; however, the Standard does not appear to require Information Security involvement prior to project approval or selection. IT management should consider whether the Project Management Standard should require Information Security involvement prior to project approval or selection so that relevant security requirements can be identified and considered earlier in the project decision-making process.
 - The Incident Response Plan has not been updated since May 2023 and was last formally updated in May 2023, despite organizational changes such as departmental and job title updates having occurred. IT management should review the Incident Response Plan and update as necessary to reflect the current organizational structure, roles, and responsibilities and should consider establishing a periodic review process to help maintain the plan's accuracy.
 - Portfolio owners rank projects quarterly using the Project Matrix; however, the quantitative project rankings are not currently tracked within ServiceNow. Tracking quantitative ranking for projects within ServiceNow may facilitate documentation and communication of project priority. IT management should consider whether capturing quantitative project rankings within ServiceNow would improve documentation, transparency, and communication of project priorities.
-
-



Nashville Electric Service

FY2027 Purchased Power

Internal Audit Report

For the Period: July 1, 2025 through June 30, 2026



CONFIDENTIAL

This report is intended solely for the use of management and the Board of Directors and should not be used for any other purpose. The Company's external auditors may be provided with a copy of this report in connection with fulfilling their responsibilities.

Nashville Electric Service

Purchased Power
Internal Audit – FY2027

Table of Contents

I. Executive Summary.....	2
II. Overview of Results	3

Report Distribution:	<u>Name</u>	<u>Title</u>
	Tabitha Beach	Interim CFO
	Kevin Phelps	Interim VP Power System Operations
	Vaughan Charles	VP Grid Transformation & Project Mgmt.
	Matt Dodd	Interim Corporate Controller
	Barry Daniel	Revenue & Rates Manager

Additional Distribution:	<u>Name</u>	<u>Title</u>
	Rob McCabe	Audit Committee Chair
	Teresa Broyles-Aplin	President & CEO
	Laura Smith	Interim EVP & Chief Legal Officer
	Trish Holliday	VP Chief People Officer
	Ron Womble	VP CIO

I. Executive Summary

Introduction

Baker Tilly Advisory Group, LP has performed certain internal audit services for Nashville Electric Service (NES) related to TVA power invoice reconciliation, voltage reduction events, and the TVA Collaborative Workspace process. Our fieldwork was performed during August 2026. The audit covered the period July 1, 2025 through June 30, 2026. Our primary objective was to independently and objectively test and assess the internal controls related to **Purchased Power**. Our services were performed in accordance with the terms of our contract with an effective date beginning on June 1, 2026. We conducted this audit in accordance with the *Global Internal Audit Standards issued by the Institute of Internal Auditors*. 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.

Scope

We evaluated the design and operating effectiveness of key controls. Areas of audit emphasis included, but were not limited to, determining whether:

- The monthly TVA power invoice is accurate and line-item amounts are reviewed timely, appropriately supported, reconciled and approved in accordance with NES policy,
- Other charges and credits per various agreements, such as Green Power Switch and Valley Investment Initiative, are properly supported and calculated on the monthly invoice, as needed,
- Payment of the monthly power invoice is reviewed and approved in accordance with NES and TVA policy, and
- Access to the TVA Collaborative Workspace is appropriately restricted.

Corporate Governance, Culture and Stewardship Considerations

We considered corporate governance, culture, and stewardship initiatives that may have an impact on the scope of the audit. We did not identify any extraordinary initiatives that had an impact on the audit scope. Inherently, many of the procedures performed in our audit are focused on governance activities.

II. Overview of Results

During the course of our work, no reportable findings were identified. The design and operating effectiveness of controls evaluated during the audit appear adequate and reasonable. However, due to inherent limitations in any system of internal control, errors or irregularities may occur and not be detected. Therefore, absolute reliance should not be placed on these controls.

We appreciate the cooperation extended to us by personnel at NES and are pleased to be of service. If there are any questions or comments regarding this report, please contact us. Contact information for the Director and Assistant Director of Internal Audit responsible for this work is presented below.

Scott Nalley, CIA, CISA, CISSP
Director of Internal Audit
615-782-4252
Scott.Nalley@bakertilly.com

Patrick Clark, CIA
Assistant Director of Internal Audit
615-921-5997
Patrick.Clark@bakertilly.com

Nashville Electric Service
4th Quarter Fiscal Year 2026 Follow-up and Remediation
September 23, 2026

Findings Noted During the FY25 Timekeeping & Payroll Audit				
Finding Description	Risk Level	Management Action Plan	Disposition	Status
2025-02 PeopleSoft User Access Review A periodic review of PeopleSoft users' access is not required to be performed, and a comprehensive review has not been performed in several years. During our review of PeopleSoft users' access as of April 2025, we identified the following: •One employee transferred from the Human Resources department to the Training department, but retained their Human Resource user role, which is not needed based on their current job responsibilities, •One employee transferred from the Accounting department to the Accounts Payable department, but retained their Accounting user role, which is not needed based on their current job responsibilities, and •Three Accounting department personnel responsible for processing payroll have a "Timekeeper" user role that allows them to edit all employees' timekeeping (hours worked) records in PeopleSoft which creates a segregation of duties conflict. We reviewed timekeeping entries processed by these individuals for the period January through June 2025 and did not identify any unusual transactions.	Medium	A comprehensive review of current PeopleSoft user roles and access privileges will be completed followed by ongoing quarterly access reviews. Target Implementation Date: June 30, 2026 Revised Implementation Date: January 31, 2027	Management is in process of implementing Oracle Time and Labor and will decommission PeopleSoft once Oracle Time and Labor is live. A comprehensive review of user access will occur as part of the Oracle Time and Labor implementation and is expected to be completed in January 2027.	Revised Target Date

Nashville Electric Service
4th Quarter Fiscal Year 2026 Follow-up and Remediation
September 23, 2026

Findings Noted During the FY25 Network & Cybersecurity - Corporate IT Audit				
Finding Description	Risk Level	Management Action Plan	Disposition	Status
2025-01 Unauthorized Applications Procedures are not adequate to detect and remove unauthorized, non-malicious software installed on network devices. One application, AutoHotkey, out of a sample of 30 applications installed on the network, was not approved for installation on network devices in accordance with IT policy. While NES uses a management detection and response tool to block the installation of malicious applications, unapproved applications that are not deemed malicious can be installed by users. IT management previously identified AutoHotkey as an application to be removed from the network; however, it was not effectively removed from all network devices.	Medium	IT will establish a formal process to perform a quarterly reconciliation of installed software against the organization's approved software list. Any applications identified as unapproved will be evaluated, and, where appropriate, removed from endpoints. In addition, IT will reinforce user awareness by providing targeted communications and training on acceptable use policies related to software installation and usage. Target Implementation Date: March 31, 2026 Revised Implementation Date: May 31, 2026 Revised Implementation Date: October 31, 2026	Management has developed an approved software list. Additional end-user communication and training will occur with Q4 Security Awareness training in October 2026, and a full reconciliation of existing software installations against the approved software list will occur at that time.	Revised Target Date

Nashville Electric Service
4th Quarter Fiscal Year 2026 Follow-up and Remediation
September 23, 2026

Findings Noted During the FY26 Environmental Safety Audit				
Finding Description	Risk Level	Management Action Plan	Disposition	Status
2026-03 Environmental Compliance Training Mandatory environmental compliance training related to Spill Prevention, Control and Countermeasure (SPCC), Polychlorinated Biphenyls (PCB)/Asbestos and Hazards Awareness, and Substation Maintenance and Structure Hazard Awareness are not always completed timely. This is a repeat audit finding from prior years. We determined the following: •Twenty-two employees of 335 did not complete the annual SPCC training in 2024. The 2025 training has not been scheduled. Once identified by Internal Audit, training sessions were scheduled to be completed by December 15, 2025. •Six of 33 employees did not complete PCB/Asbestos and Hazards Awareness training in August/September 2025. At the time of our audit, a make-up training session had not occurred, but has been scheduled for November 4, 2025. •Five of 28 employees did not complete the Substation Maintenance and Structure Hazard Awareness training in August 2025. At the time of our audit, a make-up training session had not occurred, but has been scheduled for November 4, 2025.	Medium	NES is in the final stage of contract terms and conditions agreement with Origami Risk. The planned implementation of the software configuration from a staged environment to a live application will take several months to complete. Automation surrounding employee training documentation will be included in the overall configuration. The SPCC, PCB/Asbestos and Substation Maintenance Hazards Awareness trainings have been completed as planned. Target Implementation Date: June 30, 2026 Revised Implementation Date: October 31, 2026	Implementation of the Origami Risk application has been extended to October 2026.	Revised Target Date

Nashville Electric Service
4th Quarter Fiscal Year 2026 Follow-up and Remediation
September 23, 2026

Findings Noted During the FY26 T&D Operations Audit				
Finding Description	Risk Level	Management Action Plan	Disposition	Status
2026-01 Capital Tools Tracking and Safeguarding Internal controls and policies over the acquisition, storage and recordkeeping of capital tools are not adequate to ensure that all tools are accounted for, recorded in the general ledger and adequately safeguarded. The process for communicating the purchase and retirement of capital tools was changed in the last three years, whereby, Facilities personnel would no longer provide item details to Accounting, but would continue to provide the tracking numbers (T numbers) to Service Center personnel. This change was not formally documented nor communicated to relevant parties and contributed to a breakdown in reporting the purchase and retirement of capital tools. The following control weaknesses were identified: •T numbers are not always requested by the purchaser. •T numbers are manually assigned and tracked. •Tool listings maintained by each Service Center are incomplete. We identified at least 60 tools purchased after January 1, 2021 that were above the \$1,000 capitalization threshold that were not recorded in the general ledger. •Capital tool listings maintained by the Service Centers or in the General Ledger may not include all required documentation needed for warranty purposes. •The North center does not always limit access to the locked storage room where excess tools are stored.	Medium	1.T&D Operations Managers will request the assigned T number list for all assets not currently in the general ledger from Accounting for their center and will work with their direct reports to verify if these assets exist. Going forward, the T&D Operations Managers will ensure a complete listing of all tools purchased and retired, regardless of cost, is maintained. 2.T&D Operations Managers will work with Accounting and Facilities management to define, document and communicate the process for tracking tools. 3.T&D Operations Managers along with Accounting management will define, document and communicate the policy and procedures for tracking and recording tools to be capitalized for years beginning fiscal year 2027. 4.T&D Operations management will begin an annual physical count of all tools. 5.T&D Operations Manager for the North Service Center will limit access to the excess tools storage area to the Operations Manager and Field Superintendent. 6.Facilities management will document all T number assignments and will maintain documentation per the NES Retention Policy. Revised Implementation Date: October 31, 2026	Management is working through all aspects of the remediation action plans, but has primarily been focused on storm and operational improvement efforts and recent organizational realignments. The expected implementation date for all action items has been extended to October 2026.	Revised Target Date

Nashville Electric Service
4th Quarter Fiscal Year 2026 Follow-up and Remediation
September 23, 2026

Findings Noted During the FY26 Equipment and Materials Management Audit				
Finding Description	Risk Level	Management Action Plan	Disposition	Status
2026-02 Scrap Wire Estimated Weight Calculation The scrap wire estimated weight calculation may not provide reasonable estimates which are used to solicit bids from perspective buyers, and payments received from the buyers do not always follow NES' scrap wire sale policy. We reviewed the one scrap wire sale that occurred during the audit period and determined the following: for all wire types included in this sale, the total estimated weight was 50,000 lbs. and the actual total weight was 359,659 lbs. resulting in an overall weight variance of 309,659 lbs. An initial payment in the form of a cashier's check was received from the buyer for \$77,325.00 based on the estimated weights. An additional payment in the form of a company check was received from the buyer approximately one month after the initial sale for \$490,834.30 based on actual weight information provided by the buyer. The company check was addressed to and received by the Procurement Department, whereas the policy requires checks to be addressed to NES Mail Remittance. We reviewed one additional sale that occurred prior to our audit period and determined that there was also a large variance between the estimated and actual weights for scrap wire.	Low	To improve the accuracy of scrap wire weight estimates, Supply Chain will use historical average weights by wire type when preparing estimates for future scrap wire sales. In addition, bid documents will be updated to include clear and consistent instructions for submitting payments in accordance with NES policy. Target Implementation Date: June 1, 2026 Revised Implementation Date: September 30, 2026	Due to the infrequency of scrap wire sales, management is in process of completing the first scrap wire sale since the audit was performed and is in process of revising weight estimates and payment instructions. The in-process scrap wire sale is expected to be completed by end of September 2026.	Revised Target Date

Executive Session

Miscellaneous