**Audit and Ethics Committee Meeting**

Jul 22, 2026 8:00 AM - 8:30 AM CDT

NES Board Room 121

---


1. Safety Moment - Kevin Phelps
2. Recommendation for approval of minutes of the Audit and Ethics Committee meeting held May 27, 2026
3. Internal Audit Reports - Baker Tilly - Scott Nalley
   - 3.1. Audit and Ethics Committee Calendar
   - 3.2. Internal Audit Status Report
   - 3.3. Internal Audit Report - Cybersecurity Operations
   - 3.4. Recommendations - Cybersecurity Operations
4. Internal Audit Annual Communications
   - 4.1. Internal Audit Risk Assessment
   - 4.2. Three-Year Internal Audit Plan FY27-FY28-FY29
   - 4.3. Quality Assurance Self-Assessment Report
   - 4.4. Baker Tilly Leadership Bios
5. Recommendation for approval of FY27 Internal Audit Plan, Audit and Ethics Committee Charter, Internal Audit Charter - Scott Nalley
   - 5.1. FY27 Internal Audit Plan
   - 5.2. Audit and Ethics Committee Charter
   - 5.3. Internal Audit Charter
6. Executive Session
7. Miscellaneous

**July is UV Safety Awareness Month.** While many of us enjoy spending more time outdoors during the summer, it's important to remember that UV rays can damage both our skin and eyes. Overexposure can lead to sunburn, skin cancer, cataracts, and other eye injuries.

**A few simple ways to stay protected:**

- Use broad-spectrum sunscreen with SPF 30 or higher.
- Reapply sunscreen every two hours when working or spending time outside.
- Wear sunglasses with 100% UV protection and a hat for added protection.
- Seek shade when possible, especially between 10 a.m. and 4 p.m. when UV rays are strongest.
- Remember that UV rays can penetrate clouds, so protection is important even on overcast days.

**Takeaway:** A little protection goes a long way. Protect your skin and eyes today to prevent serious health problems down the road. Stay safe and stay protected

**AUDIT AND ETHICS COMMITTEE MEETING MINUTES**
**MAY 27, 2026**

The Audit and Ethics Committee meeting was held on Wednesday, May 27, 2026.

Committee Members Present: Committee Chair Rob McCabe, Clifton Harris, Anne Davis, Casey Santos and Ian Prunty

Officers Present: Teresa Broyles-Aplin, Laura Smith, Dr. Trish Holliday, Brent Baker and Recording Secretary David Frankenberg

Committee Chair Rob McCabe called the meeting to order at 8:06 a.m.

## SAFETY MOMENT

Brad Heck presented a safety moment on how to stay safe around roadside work zones.

## MINUTES

> Upon motion by Member Davis and seconded by Member Harris, the Committee approved the minutes from the Audit and Ethics Committee meeting held April 22, 2026, with five ayes and zero nays.

## BAKER TILLY INTERNAL AUDIT REPORT

Scott Nalley and Patrick Clark provided a summary of completed internal audit services for the following audits:

- Non-Metered Electric Billing and Miscellaneous Revenue
- Equipment and Materials Management
- Contribution in Aid to Construction
- FY26 Board, Executives and Employee Accounts
- Q2 and Q3 FY26 Follow-up and Remediation

Mr. Nalley reported that seven prior audit observations were reviewed as part of the Q2 and Q3 FY26 follow-up process. Of those observations, three were determined to have been resolved, while four remain open with extended target remediation dates.

Member Davis inquired when the Winter Storm Fern expenditures audit will be completed. Mr. Clark replied that it is in progress with a completion date slated for the end of June.

## MISCELLANEOUS

There were no miscellaneous items to present.

**EXECUTIVE SESSION**

There was no Executive Session held.

**ADJOURNMENT**

The meeting adjourned at 8:20 a.m.

**APPROVED: _____**
**Committee Chair Rob McCabe**

**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 | | | September | | |
| **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 | | |
| **COMPLIANCE** | | | | | |
| Review effectiveness of system for monitoring compliance | X | X | X | X | |
| Review findings of examinations of regulatory agencies | | | | | X |

| COMMITTEE ACTIONS | 1st Qtr* | 2nd Qtr* | 3rd Qtr* | 4th Qtr* | As Needed |
|---|---|---|---|---|---|
| **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-FY26**
**As of July 22, 2026**

| CURRENT AUDITS | |
|---|---|
| **Audit Description** | **Date Started** |
| Physical Security & Employee Safety | November 2025 |
| Storm Expenditures | April 2026 |
| Meter to Cash | April 2026 |
| Network and Cybersecurity - Corporate | May 2026 |
| **UPCOMING AUDITS** | |
| **Audit Description** | **Scheduled Start Date** |
| Capital Projects and Capitalization Process | Defer to FY27 |
| **NON-AUDIT SERVICES** | |
| **Service Description** | **Status/Scheduled Date** |
| Enterprise Risk Management Assistance | Complete |
| Oracle C2M User Roles Segregation of Duties Assistance | In-Process |
| ServiceNow Integrated Risk Management (IRM) Assistance | In-Process |
| Fraud Risk Assessment | May 2026 |
| **Completed AUDITS** | |
| **Audit Description** | **Completion Date** |
| Travel Expenses | November 2025 |
| Q1 FY26 Follow-up and Remediation | January 2026 |
| Environmental Safety | March 2026 |
| T&D Operations | March 2026 |
| Non-Metered Electric Billing and Miscellaneous Revenues | May 2026 |
| Equipment and Materials Management | May 2026 |
| Contribution in Aid to Construction | May 2026 |
| Board, Executive, and Employee Accounts | May 2026 |
| Q2 & Q3 FY26 Follow-up and Remediation | May 2026 |
| Cybersecurity Operations | July 2026 |




# Nashville Electric Service

## FY2026 Cybersecurity Operations

Integrated Audit Report
For the Period: April 1, 2025 through March 31, 2026

bakertilly

**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

NE2607 Cybersecurity Operations
Integrated 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**

**V. Status of Prior Findings ..... 7**


| **Report Distribution:** | **Name** | **Title** |
|---|---|---|
| | Kevin Phelps | Interim VP Operations |
| | Landon Roeder | System Supervisor |

| **Additional Distribution:** | **Name** | **Title** |
|---|---|---|
| | Rob McCabe | Audit Committee Chair |
| | Teresa Broyles-Aplin | President & CEO |
| | Brent Baker | EVP Chief Operations & Innovation Officer |
| | David Frankenberg | VP CFO |
| | Trish Holliday | VP Chief People Officer |
| | Laura Smith | VP Chief Legal Officer & General Counsel |
| | Ron Womble | VP CIO |

# I. Executive Summary

**Introduction**

Barker Tilly Advisory Group, LP has performed certain internal audit services for Nashville Electric Service (NES) related to Cybersecurity Operations processes. Our fieldwork was performed April 2026 through May 2026. The audit covered the period from April 1, 2025 through March 31, 2026. Our primary objective was to independently and objectively test and assess the internal controls related to **Cybersecurity Operations**. 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 Generally Accepted Government Auditing Standards and the *International Standards for the Professional Practice of Internal Auditing*. 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. We also performed follow-up procedures on audit findings and recommendations issued in prior audits and company compliance reviews to ensure that remediation efforts had been performed. Areas of audit emphasis included, but were not limited to, determining whether:

- Policies and procedures are in place, documented and current,
- Physical access to Systems Operations Area is appropriately restricted and monitored,
- Administrative access to the firewall is appropriately restricted,
- The IPS is appropriately configured,
- Internal and External Firewalls are appropriately configured,
- Firewall and IPS alerts are monitored,
- Network monitoring tools are appropriately configured,
- VPN access is limited to appropriate users,
- Segmentation from the corporate network,
- Server and workstations are appropriately patched,
- Appliances are appropriately patched,
- Change management processes are appropriately followed for updates,
- Physical and environmental controls are in place for the Disaster Recovery site,
- Operations department processes corresponding to Cybersecurity Operations are functioning appropriately, in accordance with policy and procedures, and
- Prior remediation items are either resolved or in the process of remediation.

**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 |
|---|---|---|---|---|---|
| **Cybersecurity Operations:** | | | | | |
| **Operations Compliance Department** | Satisfactory | - | - | 1 | 6 |
| **Total** | | - | - | 1 | |

**Status of Prior Audit Findings**

The following table portrays the status of observations identified in the FY2022 Power System Operations review. These items represent best practices and/or recommendations to enhance operational efficiencies.

| Internal Audit Area | Risk Rating | Number of Prior Findings | Number Unresolved Findings | Page |
|---|---|---|---|---|
| **FY2022 Power System Operations:** | | | | |
| Lack of Risk-Based Categorization and Rationale of Applying Patches | N/A | 1 | 1 | 7 |
| Self-Reporting Criteria and Reporting Thresholds | N/A | 1 | - | 8 |
| Patch Ticketing System and Process Missing Key Elements | N/A | 1 | - | 8 |
| **Total** | - | **3** | **1** | |

**Conclusion Summary**

There were no high-risk issues identified during our procedures and the finding noted does 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.

Resolution of the prior audit findings are summarized in **Section V** 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: Operations Compliance Department

**Response Priority:** Low

NES employees are not always aligned with an appropriate job department. During testing of job descriptions, we identified three employees and one supervisor listed under System Operations - Test Department, who were performing job responsibilities pertaining to System Operations Compliance. Three of these employees were performing compliance activities full time and one employee was performing compliance activities part time. These employees were grouped within the System Operations Test Department as a sub department for system operations compliance employees does not exist.

**Risk:** Absorbing critical compliance functions into another department may reduce visibility into the budgetary needs, staffing, and training resources necessary for these employees' activities. The inability to staff or train employees performing NERC related compliance functions could result in compliance failures, subjecting NES to potential regulatory fines.

**Recommendation:** NES should consider creating a sub department within System Operations for compliance employees to align with their job responsibilities.

***Management's Response:*** *NES Operations will be creating sub department 4340 to address this.*

***Responsibility:*** Kevin Phelps and Landon Roeder

***Implementation Date:*** October 31, 2026

## V. Status of Prior Findings

In order to keep the Audit Committee informed of the status of prior recommendations, the following table summarizes previous findings and their status, if not previously remediated:

| Findings Noted During FY2022 Power System Operations | | | |
|---|---|---|---|
| **Issue Description** | **Risk Level** | **Disposition** | **Management Response** |
| ***Lack of Risk-Based Categorization and Rationale of Applying Patches:*** NES had not developed a formal rationale for which patches were applied and in what timeline. Also, NES did not have a process in place to score/rate a security patch based on the vulnerability(ies) that it was mitigating utilizing metrics, such as Common Vulnerability Scoring System (CVSS) and/or vendor patch ratings. NERC Standard CIP-007 (Part 2.3) requires that within 35 days of evaluation completion (determination if security patches are available), patches must either be applied, a dated mitigation plan must be created or an existing mitigation plan must be revised. Currently, all security patches are applied within the 35-day time frame, regardless of their severity or applicability to the NES environment. Additional flexibility could be achieved by | N/A | With the assistance of management, Internal Audit observed a spreadsheet created by Operations consisting of risk-based categorization and patch application rationale. This document is currently being reviewed by Operations management and is waiting to be formalized. | ***Management Response:*** *NES Operations has evaluated and documented risk exposure and impact for all compliance cyber assets. Evaluation of non-compliance cyber assets is in process.*<br><br>***Responsibility:*** *Kevin Phelps and Landon Roeder*<br><br>***Target Date:*** *October 31, 2026* |

| Findings Noted During FY2022 Power System Operations | | | |
|---|---|---|---|
| **Issue Description** | **Risk Level** | **Disposition** | **Management Response** |
| documenting a time frame rationale based on the severity of vulnerabilities associated with current patch. | | | |
| ***Self-Reporting Criteria and Reporting Thresholds:*** A threshold for self-reporting NERC CIP patch "misses" based on potential risk to the BES had not been developed or documented. Currently, any and all patch violations are self-reported, regardless of mitigating factors and potential risk to NES or the BES, and there is not specified criteria for rating potential risk to NES or the BES. | N/A | Internal Audit inquired with management and determined that Operations reevaluated environments which are subject to NERC CIP reporting. Previous environments which generated this issue are no longer subject to NERC CIP compliance. Therefore, the risk related to this issue has been reduced to an acceptable level. Management also determined that in the event an issue is identified, they will apply a conservative approach and self-report if the issue is in an environment subject to NERC compliance.<br><br>**Residual risk has been reduced to an acceptable level.** | ***N/A*** |
| ***Patch Ticketing System and Process Missing Key Elements:*** NES is not using a standard ticketing system with commonly used ticket workflows, ticket closure | N/A | Management implemented Change Gear as their Change Management Solution to serve as a standard ticketing system to facilitate change | ***N/A*** |

| Findings Noted During FY2022 Power System Operations | | | |
|---|---|---|---|
| **Issue Description** | **Risk Level** | **Disposition** | **Management Response** |
| process requirements, and linkage of ticket item with asset inventory. NES is currently using SharePoint-based ticketing, which is developed and maintained by NES operations support staff. This is a standalone system and is accessed by the NES operations support staff only. During our review, we identified the following:<br>The process to close tickets for patches implemented is informal. There is no defined process in place to verify or "sign off" that a change has been implemented prior to closing a ticket.<br>• Tickets informally use specific days of the month to identify if a change is related to NERC CIP/security patching, rather than having a field to clearly identify this.<br>• The ticketing process does not link to an asset inventory; thus, changes<br>cannot be easily linked to their affected assets. | | management workflows, ticket closure requirements, and linkage of ticket items to their asset inventory. Change Gear is also the application to document the sign-off and approval of changes, and includes notations indicating whether tickets are relevant to specific CIP requirements. Additionally, change management testing of the Change Gear application was included in the scope of the audit and no exceptions were identified.<br><br>**Issue appears resolved.** | |

# Nashville Electric Service
# FY2026 Cybersecurity Operations
# Recommendations and Best Practices

To: Kevin Phelps and Landon Roeder

From: Baker Tilly

Date: July 22, 2026

During our review covering the period 4/1/2025 through 3/31/2026, 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

- Delays in notifying Operations of retired employees with CIP access puts undue pressure on Operations to remove access within regulatory timeframes. During testing of terminated employees with CIP access, we identified one retired employee who upon their retirement, the automated HR system (HCM) sent an automated email to Operations two days after this employee's term date. NERC regulations require that CIP access be removed within 24 hours of Operations being notified of the termination. Failure to comply with NERC regulations can result in significant fines. While access for this employee was removed within 24 hours of Operations being notified, Operations management should request HR to provide the CIP Senior Manager, or VP of Operations, advance notice of upcoming retirements for employees who are flagged as CIP employees in the HR system.

- The host server for the backup application for the alpha and delta domains are currently running on the alpha and delta domain controllers. Generally, domain controller activity should be limited to authentication and directory activity. In addition, running the backup application on the domain controller would require Operations to manually rebuild the domain controllers, instead of rebuild them from a backup, in the event the server failed. Operations management should remove the backup host from the domain controllers and run them on their own servers.

- Domain password policies have minimum password age set to 0. During testing of the OT network documents, we identified that the minimum password age for Alpha, Delta, and SCADADMZ were set to zero days. While the password configurations meet or exceed the minimum requirements set by the documented NES Policy, it is an industry best practice to set the minimum age to at least 1 day to reduce the risk of employees resetting their password to meet the remembered password history and keep their previous password. Operations management should consider setting the minimum password age to at least 1 day.

- Supporting evidence of system account reviews is not always maintained. During testing of system account reviews, we inspected email evidence indicating that a system account review was performed, but supporting documentation showing the detail of the review could not be provided. Operations management should

maintain supporting evidence of system account reviews in the event a regulator requests evidence that reviews are performed in accordance with policy.

- CIP training records in Peoplesoft are not always accurate with current training information. During badge access testing, one of 82 employees inspected was identified as having last completed CIP training in December 2024. Upon further investigation, it was determined that this employee actually completed CIP training in December 2025. Operations management should ensure that all CIP training data is imported into Peoplesoft after the completion of training to support effective monitoring of training compliance.

The IIA Global Internal Audit Standards require that we discuss at least annually, certain aspects of governance of the internal audit function with the board and senior management to maintain alignment among respective responsibilities of the board, senior management, and the internal audit function. In the spirit of these communications, we affirm that:

- The purpose of internal auditing is to help strengthen the organization's ability to create, protect, and sustain value by providing the board and management with independent, risk-based, and objective assurance, advice, insight, and foresight,
- The Internal Audit function is established, approved, and supported by the board,
- The Internal Audit function's authority, purpose, roles, independence, access rights, responsibilities, and services (i.e., Internal Audit Mandate) are documented in the Internal Audit Charter,
- The Internal Audit Charter is approved by the board and senior management,
- The Internal Audit Director provides the board and senior management with information needed to support the internal audit function throughout the organization,
- The Internal Audit function is positioned independently,
- The Internal Audit Director maintains and enhances the qualifications and competencies needed to fulfill the roles and responsibilities expected by the board and senior management, and
- The Internal Audit function is overseen by the board and provides sufficient communications to the board and senior management regarding the sufficiency of internal audit resources, potential impairments to independence, results of internal audit services, and results from internal and external quality assurance assessments and improvement programs.

**Internal Audit Plan**

We updated the prior year's risk assessment by interviewing key members of management including board members, the CEO, EVP, CFO, CIO, and all VPs.

Adjustments were made to scoring for a few risk areas which resulted in Vegetation Management moving from a medium to high ranking, IT Strategy moving from a high to medium ranking and all other risk areas adjusted remained within the previously assessed risk range (high, medium, or low). One new risk area, Emergency Response Planning was added and the risk rating was determined to be medium. The risk assessment is included in the materials for your review.

During our interviews with NES leadership, several recurring enterprise level themes emerged. These themes are summarized for informational purposes and will be considered during the course of planned internal audit projects. Risk and opportunity themes mentioned across the organization included:

- Strengthening operational readiness and emergency response plans,
- Incident command structure maturity,

- Infrastructure modernization activities,
- Vegetation management programs, and
- Leveraging and enhancing use of existing technologies in operations and customer-facing activities.

Also, we reviewed the results of the winter storm Fern after-action review and have considered those observations and recommendations from that report in the development of our audit plan and/or the scope of individual audits. The FY27 audit plan includes enhancements to the Enterprise Risk Assessment (ERM) program to address recommendations in the after-action review report.

Fiscal year 2026 was the final year of the three-year plan proposed in June 2023. Consistent with our prior methodology, this year's risk assessment was used to develop a new three-year audit plan that covers fiscal years 2027, 2028, and 2029. The FY27 audit plan includes 6,990 hours. The three year proposed internal audit plan is included in the materials for your review.

**Effectiveness of the Internal Audit Function**

The Internal Audit activity at NES is outsourced to help ensure independent assurance and consulting services to help improve the organization as a whole. Internal Audit must continuously adapt to organizational objectives as they change. To provide the best service possible to the organization, the following strategic objectives have been identified:

- Maintain a working knowledge and appropriate level of awareness to changing management objectives,
- Understand the industry and how changes to the industry could affect the organization,
- Continuously provide value to the organizations through consulting and process improvement opportunities,
- Maintain a positive relationship with auditees and members of management, and
- Practice continuous improvement of the internal audit activity to improve efficiency and effectiveness.

***Evaluation by the Audit Committee***

The Committee should evaluate IA's effectiveness based on the following IIA performance standards:

- **Management of the Internal Audit Function:** Management is effective when the work achieves the purpose and responsibility included in the IA Charter; the IA activity conforms to the definition of internal auditing; and individuals who are part of the IA activity demonstrate conformance with the Code of Ethics.
- **Planning:** There must be a risk-based audit plan to determine the priorities of the IA activity, consistent with the organization's goals.
- **Communication and Approval:** The plans and resource requirements must be communicated for review and approval, as well as the impact of any resource limitations.
- **Resource Management:** IA resources must be appropriate, sufficient, and effectively deployed to

achieve the approved plan.

- **Policies and Procedures:** There must be established policies and procedures to guide the IA activity.
- **Coordination:** Information should be shared, and activities coordinated with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.
- **Reporting to Senior Management and the Board:** IA must report periodically to senior management and the Board on the IA activity's purpose, authority, responsibility, and performance relative to the IA plan. Reporting must include significant risk exposures and control issues.
- **External Service Provider & Organizational Responsibility for IA:** Because we are an external service provider, you must be aware of your responsibility for maintaining an effective IA activity.

The Audit & Ethics Committee adopted a standard set of questions to be used by the Committee to assess the effectiveness of the internal audit function. The questions were reviewed and updated in consideration of the IIA Global Internal Audit Standards effective January 2025. These questions will be distributed to the members of the Committee subsequent to this meeting with the results to be presented at the next Audit and Ethics Committee meeting.

***Ongoing Evaluation by Management***

We have adopted a Quality Assurance and Improvement Program that includes individual audit performance surveys completed by NES management and VPs. Individual audit survey results for fiscal year 2026 projects to date are favorable. Respondents were asked to rate the quality of our service on a scale of 1-5 in six performance areas, with 5 being the highest ranking. For all survey responses received the average score for each question was **4 or above** in all areas, with an **overall average score of 4.8** which is consistent with the prior year.

**Compliance with the IIA Global Internal Audit Standards**

In 2024, the IIA performed a quality review of the internal audit function. Their review was performed to assess the internal audit function's compliance with internal auditing standards. The IIA determined that the internal audit activity generally conforms to the standards. This is the highest rating given by the IIA. Baker Tilly has continued to follow the same practices that were in place at the time of the quality review. The next external quality review will be performed in 2027.

In June 2026, we completed a self-assessment to evaluate our compliance with the internal audit standards and we obtained feedback from NES executives and Baker Tilly team members using surveys to assess our overall performance for fiscal year 2026. Survey respondents were asked to rate the quality of our performance on a scale of 1-5 with 5 being the highest ranking. For all survey responses received the **overall average score was 4.6 and 4.7** from NES executives and Baker Tilly team members, respectively. Through the self-assessment process, we identified areas of improvement and developed action plans to address those needs. We determined that the internal audit activity is generally achieving compliance with the standards. The results of our internal quality self-assessment are included in the materials for your review.

**Organizational Independence**

According to the IIA Global Internal Audit standards, the Director of Internal Audit must confirm to the Audit Committee annually that there is organizational independence for the IA activity. First, IA reports to a level within the organization that allows fulfillment of responsibilities by reporting administratively to the CEO and functionally to the Audit Committee. Second, the IA function has been free from interference in determining the scope of internal auditing, performing work, and communicating results. Finally, IA communicates and interacts directly with the Audit Committee. These conditions allow IA to have an impartial, unbiased attitude, and avoid any conflict of interest. Accordingly, we can confirm organizational independence.

**Appointment and Compensation of the Internal Audit Firm**

In April 2026, the Board approved a new contract effective June 1, 2026. The contract between NES and Baker Tilly Advisory Group, LP for Internal Audit services is a five-year contract.

The Committee is responsible for appointment and assessment of the qualifications of the Internal Audit Director (i.e., Chief Audit Executive), and approval of their roles and responsibilities. Competencies and qualifications of the Chief Audit Executive typically include:

- A comprehensive understanding of the Global Internal Audit Standards and leading internal audit practices,
- Experience building and managing an effective internal audit function by recruiting, hiring, and training internal auditors and helping them develop relevant competencies,
- Certified Internal Auditor designation or other relevant professional education, certifications, and credentials,
- Leadership experience, and
- Industry or sector experience.

The Baker Tilly Risk Assurance Services executive and management team members in charge of NES' IA activity average more than 15 years of experience in the audit and accounting fields, with emphasis in Information Technology and Cybersecurity. Credentials held include the following designations: Certified Public Accountant (CPA), Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), Certification Information Systems Security Professional (CISSP), and Certified Information Technology Professional (CITP), as well as others. Each team member is required to obtain at least 40 hours of continuing professional education every year. Bios for management team members in charge of the NES IA activity are included in the materials for your review.

The internal audit team also includes resources provided by a minority-owned subcontractor, SB & Company, LLC.

We confirm that the acting Internal Audit Director has the desired competencies and qualifications. We

also confirm that Baker Tilly and SB & Company, LLC are able to provide sufficient staff with the appropriate qualifications and experience to meet the expectations of the Committee as outlined in the Internal Audit Charter. Where additional expertise is required, internal audit utilizes other Baker Tilly experts or contracts with other third parties.

**Audit & Ethics Charter and Internal Audit Charter**

Both the Audit & Ethics Committee and the Internal Audit charters have been reviewed in consideration of the IIA Global Internal Audit standards, and we do not recommend any changes. Both charters are included in the materials for your review.

**Nashville Electric Service**
**2026 Audit Risk Assessment**
**(preparation for FY 2027 Internal Audit Plan)**

| Risk Area | Risk Area Description | Risk Score | Risk Ranking | Audit Frequency |
|---|---|---|---|---|
| Cybersecurity (Operations) | Protecting the Operations network from electronic crime such as network outages, data compromised by hackers, computer viruses, and lack of security patches. Includes preventing, detecting, and responding to cyber threats. | 5.40 | High | Annual |
| Cybersecurity (Corporate) | Protecting the Corporate network from electronic crime such as network outages, data compromised by hackers, computer viruses, and lack of security patches. Includes preventing, detecting, and responding to cyber threats. | 5.30 | High | Annual |
| Metered Electric Billing | Calculating, reviewing and issuing bills to customers for electric usage tracked using a meter. This includes residential, commercial and manufacturing customers. | 5.25 | High | Annual |
| Network Security and Data Governance | Protecting information on the network from unauthorized modification, destruction, or disclosure. Including accountability for how data is collected, classified, accessed, retained, and used across all systems including artificial intelligence (AI). This includes logical (e.g., firewalls, passwords) and physical (e.g., controlling access to the data center) security. It also includes the user provisioning process for adding, changing, and removing users from the network. | 5.15 | High | Annual |
| Vegetation Management | Tree trimming and other vegetation controls to prevent damage to electrical lines and equipment. | 5.05 | High | Annual |
| North American Electricity Reliability Corporation (NERC)/ Southeastern Electricity Reliability Corporation (SERC) | Ensuring compliance with NERC/SERC requirements. NERC develops electric reliability standards and SERC enforces the standards for the region in which TVA and NES operate. | 4.95 | High | Annual |
| Timesheet Process | Documenting, calculating and approving the number of hours an employee works. This is used to both determine the amount to pay an employee and the amount of labor cost to allocate to work orders. | 4.90 | Medium | Every 2 Years |
| Contribution in Aid to Construction/Construction Invoicing | Calculating the amount of additional revenues a change in a customer's service will provide in order to determine the amount of construction costs in excess of NES' standard level of service that the customer must pay. This also includes invoicing the customer for the amount they must pay NES for the additional construction costs. | 4.85 | Medium | Every 2 Years |

* Audit frequency is not applicable, the risk will be considered as part of all audits performed.
** The Electric Power Board has requested that the Risk Area be audited annually.

**Nashville Electric Service**
**2026 Audit Risk Assessment**
**(preparation for FY 2027 Internal Audit Plan)**

| Risk Area | Risk Area Description | Risk Score | Risk Ranking | Audit Frequency |
|---|---|---|---|---|
| Financial Reporting (General Ledger) | The primary accounting record used to track all financial transactions and prepare financial statements. This consists of the Ellipse and Flexi systems. | 4.85 | Medium | Every 2 Years |
| Emergency Response Plan | Developing and initiating standardized plans used to organize responses during emergencies such as storms, flooding, other natural disasters, and large scale incidents. Including communication, defined roles, efficient coordination across departments and agencies, and post incident monitoring. | 4.85 | Medium | Every 2 Years |
| Reliability and Capacity Planning | Developing and implementing a plan for maintaining the current level of service to its customers and having the capacity to handle new customers as Nashville grows. Including strategic undergrounding, battery storage, and renewables. | 4.80 | Medium | Every 2 Years |
| Work Order Capitalization | Identifying capital costs charged to work orders and properly classifying and calculating depreciation costs for accurate financial statement presentation. | 4.80 | Medium | Every 2 Years |
| Application Change Management Process | The sequence of steps or activities that are followed to apply changes to applications to ensure the integrity of the related data and processes. | 4.70 | Medium | Every 2 Years |
| Supervisory Control and Data Acquisition (SCADA) system | The SCADA system is the software and network components that allow NES to monitor and manage the electric grid. | 4.70 | Medium | Every 2 Years |
| Accounts Receivable and Collections | Tracking, collecting, and recording payments due to NES for services provided, including electric power, construction, pole attachments, etc. | 4.60 | Medium | Every 2 Years |
| Work Order Process | Creating, processing, and closing work orders for utility plant construction projects (e.g., installing a new pole). Ellipse is the system in which work orders are processed. | 4.60 | Medium | Every 2 Years |
| Electrical Infrastructure Maintenance & Replacement | Developing and implementing a plan for maintaining the electrical grid and its components (poles, transformers, sub-stations, etc.) | 4.60 | Medium | Every 2 Years |
| Accounts Payable and Disbursements | Recording, tracking and issuing payments for amounts payable to vendors, suppliers and service providers. This includes controlling and setting-up vendors for payment. | 4.50 | Medium | Every 2 Years |

* Audit frequency is not applicable, the risk will be considered as part of all audits performed.
** The Electric Power Board has requested that the Risk Area be audited annually.

**Nashville Electric Service**
**2026 Audit Risk Assessment**
**(preparation for FY 2027 Internal Audit Plan)**

| Risk Area | Risk Area Description | Risk Score | Risk Ranking | Audit Frequency |
|---|---|---|---|---|
| Shadow Information Technology Groups | IT functions and activities that are not visible to or controlled by the CIO including unauthorized use of technology, which may include hardware, software, resources and cloud services, by employees within the organization. Additionally, known functions within the organization that are not overseen or managed by the CIO may not adhere to the organization's IT governance policies and control procedures. | 4.50 | Medium | ALL* |
| Termination/Retirement Process and Post-employment Benefits | Processing retirement paperwork, including calculation of retirement benefits, and managing retiree benefits post-employment. | 4.50 | Medium | Every 2 Years |
| Standard Unit Costing (Compatible Units) | Calculating, monitoring and adjusting the standard cost, including materials and labor, of performing a task (e.g., installing a pole). The standard cost is used in estimating the cost of a work order and capitalizing the resulting asset for accounting purposes. | 4.50 | Medium | Every 2 Years |
| Disconnect/Reconnect | Disconnecting service for customers who are past due on their customer account or no longer need service and reconnecting service for customers who were previously disconnected. | 4.45 | Medium | Every 2 Years |
| Physical Security | Security of buildings, sub-stations, and equipment for the protection of NES' employees, customers, and the electric grid. | 4.45 | Medium | Every 2 Years |
| IT Strategy | Designing and implementing a plan that drives the IT direction for NES, including the types of hardware and software that will be used and the level of integration of the systems to achieve NES' mission. | 4.45 | Medium | Every 2 Years |
| Customer Deposits | Collecting upfront payments from new customers to cover potential loss if a customer does not pay NES for services provided. | 4.35 | Medium | Every 2 Years |
| Purchased Power | Calculating and paying TVA for the amount of power NES uses and delivers to its customers. There are many factors in the power invoice from TVA including various program credits. | 4.35 | Medium | Every 2 Years |
| Voltage Management\Distribution Management | Monitoring and managing the amount of voltage on the system to ensure adequate service is provided to NES customers. This includes managing the voltage during periods of high demand. | 4.35 | Medium | Every 2 Years |

* Audit frequency is not applicable, the risk will be considered as part of all audits performed.
** The Electric Power Board has requested that the Risk Area be audited annually.

**Nashville Electric Service**
**2026 Audit Risk Assessment**
**(preparation for FY 2027 Internal Audit Plan)**

| Risk Area | Risk Area Description | Risk Score | Risk Ranking | Audit Frequency |
|---|---|---|---|---|
| Employee Safety/Drug Testing/Driver Requirements (CDL) | Ensuring safety of employees, contractors, customers and the general public during NES business operations. This includes ensuring that employees and contractors are qualified and capable of performing a job that could cause harm to themselves or the public. | 4.30 | Medium | Every 2 Years |
| Payroll | Paying employees for time worked at the appropriate rate, including overtime or other differentials. This includes ensuring that payroll tax and other payroll withholdings are remitted to the appropriate party timely. | 4.30 | Medium | Every 2 Years |
| Business Continuity and Disaster Recovery Planning | Developing and testing procedures to ensure NES can continue critical business operations in the event of an internal or external disaster. | 4.30 | Medium | Every 2 Years |
| Facility Construction Projects | Any construction cost related to maintenance, remodeling or expansion of existing buildings or development and construction of new buildings, such as a new service center. | 4.30 | Medium | Every 2 Years |
| Outage Reporting Process | Reporting and responding to electric power outages. | 4.30 | Medium | Every 2 Years |
| Meter Reading | Reading meters and uploading readings into the Oracle Utilities (Customer To Meter) System for billing purposes. This includes all methods of reading meters (e.g., manual, remote) and systems used in the process (MV-RS). | 4.25 | Medium | Every 2 Years |
| Meter Testing & Quality Control | Ensuring that newly purchased meters are working properly upon receipt and installed meters are operating within NES and American National Standards Institute (ANSI). | 4.25 | Medium | Every 2 Years |
| Debt Management (Bond Issuance, etc.) | Managing the process for issuing debt in accordance with NES policy and applicable laws and regulations. | 4.25 | Medium | Every 2 Years |
| Equipment & Storeroom Inventory | Recording, controlling and counting equipment and materials owned by NES. | 4.20 | Low | Every 3 Years |
| Capital Expense Classification | Budgeting and accurately classifying capital purchases (e.g., buildings, equipment, infrastructure components) | 4.15 | Low | Every 3 Years |
| Environmental Safety | Preventing adverse environmental incidents such as oil or gas spills, including clean-up and reporting these events when necessary. | 4.10 | Low | Every 3 Years |
| Key Employee Issues | Planning needed to limit organizational impact of losing a key member of the NES team that holds a large amount of knowledge related to a significant department or process. | 4.10 | Low | ALL* |

* Audit frequency is not applicable, the risk will be considered as part of all audits performed.
** The Electric Power Board has requested that the Risk Area be audited annually.

**Nashville Electric Service**
**2026 Audit Risk Assessment**
**(preparation for FY 2027 Internal Audit Plan)**

| Risk Area | Risk Area Description | Risk Score | Risk Ranking | Audit Frequency |
|---|---|---|---|---|
| Staffing | The ability to staff the department with professionals capable of servicing the needs of NES. This includes total number of professionals along with their qualifications, and succession planning. | 4.10 | Low | ALL* |
| Investments | Investing cash on hand in accordance with applicable laws and regulations. | 4.10 | Low | Every 3 Years |
| Regulatory Compliance | Compliance with existing regulatory requirements (e.g., Civil Rights, ADA, FLSA, FMLA, HIPAA, OSHA, TOSHA, EPA, FERC, GASB, IRS, Sales and Use tax, data privacy). | 4.05 | Low | ALL* |
| Corporate Governance, Culture, Stewardship | Ensuring that the company has adequate oversight and tone at the top to achieve organizational objectives and influence compliance with regulations, policies, and the code of ethics. Creating a culture that encourages responsible behavior, creates trust, promotes employee and public safety, prioritize service reliability and supports vulnerable customers, and empowers employees fostering a culture of respect and innovation. Creating customer confidence through a focus on ethical, social, environmental, cultural, and economic impacts of the organization (e.g., electric vehicles, charging stations, energy efficiency programs, customer response, employee and contractor diversity programs). | 3.95 | Low | Every 3 Years |
| Sales Tax Management | Ensuring that sales tax is applied to customers bill at the correct rate and collections are remitted to the state of TN timely. | 3.95 | Low | Every 3 Years |
| Meter Installation and Repair | Installing and repairing meters to ensure that customer usage can be accurately tracked and billed timely. | 3.90 | Low | Every 3 Years |
| Requisition Process | Requesting, approving and processing purchase requisitions for materials or services from vendors. This includes, but is not limited to, documenting and approving reasons for using a sole source or sole brand. | 3.90 | Low | Every 3 Years |
| Vendor Contract Management | Developing and executing contracts with vendors for materials and services, and monitoring to ensure vendor compliance with contract terms. | 3.90 | Low | Every 3 Years |
| Hiring Process (Internal and External) | Hiring and filling job openings with qualified candidates timely and in accordance with federal guidelines, NES policy, etc. | 3.90 | Low | Every 3 Years |
| Conflict of Interest Process | Employees reporting relationships that could create a potential conflict and negatively impact NES' business. This also includes the process for reviewing reported conflicts and managing as determined necessary. | 3.85 | Low | Every 3 Years |

* Audit frequency is not applicable, the risk will be considered as part of all audits performed.
** The Electric Power Board has requested that the Risk Area be audited annually.

**Nashville Electric Service**
**2026 Audit Risk Assessment**
**(preparation for FY 2027 Internal Audit Plan)**

| Risk Area | Risk Area Description | Risk Score | Risk Ranking | Audit Frequency |
|---|---|---|---|---|
| Non-Metered Electric Billing | Calculating, reviewing and issuing bills to customers for electric usage not tracked with a meter (e.g., street lights). | 3.85 | Low | Every 3 Years |
| Pole Attachments | Tracking and billing customers for non-electric lines and equipment attached to poles for the benefit of individuals or the community. This includes phone and cable TV lines paid for by large companies and a variety of items (e.g., speakers) paid for by small companies or individuals. | 3.85 | Low | Every 3 Years |
| Policy and Procedure Documentation and Update | Documenting, updating and communicating NES policies to ensure the consistent performance of processes and consistent treatment of customers. Documenting and communicating business processes to the individuals responsible for performing the function to ensure that business operations continue effectively and efficiently. | 3.85 | Low | ALL* |
| IT Asset Maintenance & Replacement | Ensuring that IT equipment is current (i.e., not obsolete) and capable of meeting the needs of NES. | 3.85 | Low | Every 3 Years |
| Customer Assistance Programs | Administering customer assistance programs (e.g., Home Uplift, Project Help). | 3.80 | Low | Every 3 Years |
| Plant Fixed Asset Inventory | Controlling, recording, depreciating and accounting for utility plant fixed assets. Utility plant fixed assets are the structures and components that allow NES to provide electricity to its customers. | 3.80 | Low | Every 3 Years |
| Payment In-Lieu of Taxes | The arrangement between NES and the Davidson County Metropolitan government for NES to compensate Metro government for some or all of the tax revenue that it loses because of the nature of the ownership/use of NES' property (i.e., foregone property tax revenue). | 3.75 | Low | Every 3 Years |
| Property and Right of Way Lease Agreements | Agreements that NES maintains with various individuals and organizations for installing poles and other components of the electrical grid. | 3.75 | Low | Every 3 Years |
| Customer Loan Program | Tracking and collecting loan payments from customers and passing those on to TVA. TVA makes loans to customers that meet specific requirements and NES is responsible for collecting the loan payments through the billing process. | 3.70 | Low | Every 3 Years |
| Personnel Management | Ongoing development of NES personnel, including, but not limited to, training, performance appraisals, grievances, and compensation. In addition, ongoing communication and engagement with employees. | 3.70 | Low | Every 3 Years |

* Audit frequency is not applicable, the risk will be considered as part of all audits performed.
** The Electric Power Board has requested that the Risk Area be audited annually.

**Nashville Electric Service**
**2026 Audit Risk Assessment**
**(preparation for FY 2027 Internal Audit Plan)**

| Risk Area | Risk Area Description | Risk Score | Risk Ranking | Audit Frequency |
|---|---|---|---|---|
| Customer Contract Management | Issuing and maintaining contractual agreements with customers for services provided. This includes contracts for customers with more than 50kW of electric usage, pole attachments, etc. | 3.65 | Low | Every 3 Years |
| Bank Reconciliations | Ensuring that all monies received and paid out by NES are tracked and controlled. | 3.55 | Low | Every 3 Years |
| Fleet Maintenance and Replacement | Procuring and maintaining vehicles and other similar equipment. | 3.55 | Low | Every 3 Years |
| Material Requisition and Management | Purchasing, tracking and controlling materials used by NES. This includes ensuring that adequate materials (both quantity and quality) used regularly are on hand to meet business needs in a timely manner (e.g., poles, wire). | 3.45 | Low | Every 3 Years |
| Bad Debt | Process for collecting and/or writing-off customer account balances for which the customer is unwilling or financially unable to pay. | 3.40 | Low | Every 3 Years |
| Petty Cash | Managing cash maintained on-hand to pay for miscellaneous goods or services. | 3.30 | Low | Every 3 Years |
| Board, Executive, and Employee Accounts | Ensuring that members of NES management and staff do not or cannot receive free or reduced cost of services provided by NES. | 3.30 | Low | Annual** |
| Employee Benefits | Managing and providing health insurance, time off and other benefits to employees. | 3.30 | Low | Every 3 Years |
| Travel Expenses | Ensuring that travel costs for members of NES management and staff do not personally benefit the traveler above and beyond the needs of NES. | 3.30 | Low | Annual** |
| Customer Setup and Maintenance | Setting up customers in the Oracle Utilities (Customer To Meter) system to ensure customers are billed at the correct rate, location and have the financial ability to pay for requested services. | 3.25 | Low | Every 3 Years |
| Grant Compliance | Administration of programs funded through grant opportunities, including but not limited to, preparing grant proposals, funds management, expenditure approval, and regulatory reporting, | 3.20 | Low | Every 3 Years |
| Asset Damage Billing | Identifying, calculating, and processing invoices to businesses or individuals who have damaged NES equipment. Billing for damage to NES property includes intentional damage, such as meter tampering, or accidental damage, such as hitting a pole with a vehicle. The risk area also includes evaluating, and processing payments to repair or replace property damaged by NES. | 3.15 | Low | Every 3 Years |

* Audit frequency is not applicable, the risk will be considered as part of all audits performed.
** The Electric Power Board has requested that the Risk Area be audited annually.

**Nashville Electric Service**
**2026 Audit Risk Assessment**
**(preparation for FY 2027 Internal Audit Plan)**

| Risk Area | Risk Area Description | Risk Score | Risk Ranking | Audit Frequency |
|---|---|---|---|---|
| General Fixed Asset Inventory | Recording, tracking, and depreciating capital assets such as computers, tools, desks, etc. | 3.15 | Low | Every 3 Years |
| Budgeting & Forecasting | Preparing and approving annual budgets. Monitoring and managing budget to actual, including forecasting, review and approval of changes. | 2.85 | Low | Every 3 Years |
| Contractor Management | Monitoring, onboarding, and termination of contract workers in accordance with NES policy and contractual obligations. | 2.70 | Low | Every 3 Years |
| Expenditures Related to Community Involvement | Managing funds expended for community involvement ensuring that electric revenues are not used for this purpose and does not directly benefit an NES employee. | 2.55 | Low | Every 3 Years |

*This risk will be considered as part of all audits performed.
**The Electric Power Board has requested that the Risk Area be audited annually.

**Nashville Electric Service**
**Proposed 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 |
| Internal Control Framework Assistance | | 150 |
| ERM Assistance | | 375 |
| Follow-up and Remediation-Quarterly | | 250 |
| **Total FY27 Audit Plan Hours** | | **6,990** |

| | | |
|---|---|---|
| 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 |

**Nashville Electric Service**
**Proposed Audit Plan - Fiscal Year 2028**

| Audit Description | Audit Type | Hours |
|---|---|---|
| Cybersecurity Operations | Integrated | 350 |
| Board, Executive, and Employee Accounts | Operational | 110 |
| Travel Expenses | Operational | 75 |
| Network and Cybersecurity - Corporate | IT | 625 |
| Physical Security & Employee Safety | Integrated | 400 |
| Metered Electric Billing and Customer Relations | Integrated | 850 |
| Accounting Processes | Integrated | 800 |
| Contribution In Aid to Construction | Integrated | 400 |
| NERC/SERC Reporting and Compliance | Integrated | 325 |
| Grant Administration and Stewardship Program Management | Integrated | 450 |
| Employee and Contractor Management (Hiring, Terminations, Benefits) | Integrated | 650 |
| Budgeting & Forecast | Integrated | 300 |
| Center of Excellence - Operations | Integrated | 500 |
| **Additional Items** | | |
| Planning, Administration, and Consulting | | 350 |
| Internal/External Quality Assurance and Improvement Program | | 175 |
| Audit Committee and Board Meetings | | 100 |
| Risk Assessment | | 100 |
| Internal Control Framework Assistance | | 150 |
| ERM Assistance | | 40 |
| Follow-up and Remediation | | 250 |
| **Total FY28 Audit Plan Hours** | | **7,000** |

**Nashville Electric Service**
**Proposed Audit Plan - Fiscal Year 2029**

| Audit Description | Audit Type | Hours |
|---|---|---|
| Cybersecurity Operations | Integrated | 350 |
| Board, Executive, and Employee Accounts | Operational | 110 |
| Travel Expenses | Operational | 75 |
| Network and Cybersecurity - Corporate | IT | 625 |
| Equipment and Material Management | Integrated | 500 |
| Meter to Cash | Integrated | 700 |
| Environmental Safety | Integrated | 300 |
| Timekeeping and Payroll | Integrated | 600 |
| Vegetation Management Lifecycle | Integrated | 600 |
| Non-Metered Electric Billing and Miscellaneous Revenues | Integrated | 500 |
| Infrastructure Design, Construction, and Capitalization | Integrated | 575 |
| Purchased Power and TVA Programs | Integrated | 375 |
| Work Order Life Cycle | Integrated | 440 |
| **Additional Items** | | |
| Planning, Administration, and Consulting | | 350 |
| Internal/External Quality Assurance and Improvement Program | | 100 |
| Audit Committee and Board Meetings | | 100 |
| Risk Assessment | | 125 |
| Internal Control Framework and GRC/IRM Assistance | | 250 |
| ERM Assistance | | 75 |
| Follow-up and Remediation | | 250 |
| **Total FY29 Audit Plan Hours** | | **7,000** |

# Nashville Electric Service
# Internal Quality Self-Assessment
# June 2026

To: Audit Committee

From: Internal Audit (Baker Tilly)

Date: July 22, 2026

In accordance with Nashville Electric Service (NES) Internal Audit Protocols, Internal Audit (IA) performed a self-assessment of their policies, procedures, and practices. The intent of the assessment was to assess the audit activity's compliance with the Institute of Internal Auditor's (IIA) Global Internal Audit Standards (GIAS) and the NES Internal Audit Protocols. We determined that the NES Internal Audit activity demonstrates **General Achievement** of the GIAS and NES Internal Audit Protocols.

The self-assessment was conducted using the IIA's Quality Assessment Manual (QAM) by a Baker Tilly Senior Manager who is familiar with but does not routinely work on NES audit projects. The assessment included the following elements:

- Completion of QAM Planning Guides (A1 - A6),
- Review of surveys completed by NES management and Internal Audit Staff (B1 and B2),
- Review of individual job surveys completed by NES staff and/or management,
- Review of the prior external quality assessment (October 2024), protocols, charters, and a sample of audit workpapers,
- Assessment of conformance with domains 1-5 including fieldwork and work papers (D1-D6), and
- Completion of the ratings, conclusions, and assessment herein (E1 and E2).

**Survey Summary**

The management survey was sent to 11 individuals of upper management with 8 responses received (73% response rate). The internal audit personnel survey was sent to 8 individuals with 7 responses received (88%, response rate). There was a 97% positive response rate. The ratings were based on a 5-point scale - 5 being Strongly Agree and 1 being Don't know.

Management Survey Average: 4.63

Internal Audit Personnel Survey Average: 4.72

**Survey Feedback Themes**

The themes below were derived from the written feedback included with survey responses:

- Strengths: strong business partnership and collaboration, trust, value, knowledge, relationships, professionalism, risk insight, and independence
- Opportunities: increased use of data analytics, AI, emerging risk focus, training, and planning

**Assessment Results**

The QAM defines four possible quality ratings; Full Achievement, General Achievement, Partial Achievement, or Nonachievement. The overall conclusion of the 2026 self-assessment:

- **General Achievement** – The internal audit function is not fully achieving at least one principle, standard or requirement or aspect of Domain I but is achieving the principle, standard or Purpose of Internal Auditing.

The following recommendations relevant to enhanced compliance with the standards and internal audit function maturity were identified and we expect to fully address these items by December 31, 2026:

- In 2025 both the IIA and Government Accountability Office (GAO) released new auditing standards that apply to NES internal audit. Internal audit management should continue to review and align practices to ensure that practices continue to comply with both sets of standards. In addition, internal audit management should ensure that the actions to be performed, frequency, and standards to be covered during quality assurance and improvement program activities are clearly defined and aligned with both sets of standards.

- IIA Standards require that when internal auditors are unable to conform with a requirement, a description of the circumstances and alternative actions should be documented. While the internal audit protocols generally outline alternative actions, the specific standard and circumstances driving the alternative approach are not clearly documented. Internal audit management should evaluate relevant individual requirements and ensure the circumstances are documented in accordance with the standards.

- Remediation items identified during quality assurance and improvement program activities, including self-assessments, and external quality assessments, should be documented and tracked along with follow-up and remediation items identified during the course of audit engagements.

- While an internal audit strategy has been documented, internal audit management should consider enhancing the strategy to include long-term goals and objectives, and develop key performance indicators to track success factors.

- While inherent to the audit approach, documentation of the metrics used by the audited entity to measure performance against goals and objectives is not always clearly documented. During the course of an internal audit project, the internal auditors should perform procedures to identify, document, and audit against metrics used by the audited entity to assess successful achievement of goals and objectives. If the audit entity does not have documented performance metrics, the auditors should assess need for performance metrics and make recommendations where necessary.

PRINCIPAL

# Scott Nalley, CPA, CITP, CIA, CISA, CISSP

*Scott Nalley is a principal with Baker Tilly's risk advisory practice.*




**Baker Tilly US, LLP**

555 Great Circle Road
Nashville, TN 37228
United States

**T:** +1 (615) 782 4252
scott.nalley@bakertilly.com

**bakertilly.com**


## Education

Bachelor of Business Administration in accounting
University of Memphis

Scott has more than 20 years of experience helping clients manage financial, technology, operational and regulatory risk by providing complex risk management, internal control and compliance engagements for clients in heavily regulated industries such as power and utilities, manufacturing, healthcare and governmental. Scott leads a team that provides services including internal and IT audits, network security and vulnerability assessments, data privacy evaluations, enterprise risk management (ERM) and fraud investigations.

## Specific experience

- Leads the fully outsourced and integrated internal audit team for the 12th largest public power utility and a large family-owned snack food manufacturer
- Conducts SOC 1, SOC 2 and SOC 3 examinations
- Conducts cybersecurity assessments, including evaluation of controls against common cybersecurity frameworks such as Center for Internet Security (CIS) Top 18, National Institute of Standards and Technology (NIST), Health Insurance Portability and Accountability Act (HIPAA), Health Information Trust Alliance (HITRUST)
- Collaborates with senior management and the board of directors to provide best practices for designing and implementing controls to protect organizational value
- Lead the internal control workstream for a large customer information system implementation, advising on appropriate internal controls, application controls and development of user profiles to ensure appropriate segregation of duties
- Conducted an audit of a multibillion-dollar stadium construction project
- Assisted with the development of policy and procedures
- Conducted multiple fraud investigations including a scheme to steal more than $600,000 through the check request and corporate credit card process
- Assisted with the development and implementation of an ERM application
- Assisted with the evaluation of potential conflicts of interest and the development of mitigation strategies
- Conducted internal audit quality assurance reviews in accordance with the IIA standards
- Previous board member and treasurer for local nonprofit

## Industry involvement

- American Institute of Certified Public Accountants (AICPA)
- Tennessee Society of Certified Public Accountants (TSCPA)
- Institute of Internal Auditors (IIA)
- Information Systems Audit and Control Association (ISACA)
- Tennessee State University, Accounting Advisory Board

## Thought leadership

- IIA East Tennessee Chapter, “Auditing accounts payable from an IA and fraud examiner perspective”
- Public Utility Accountant Association, “Effective internal controls”
- Middle Tennessee Association of Certified Fraud Examiners, Lipscomb Accounting Conference, TSCPA Nashville Chapter “Fraud: when truth is stranger than fiction”
- Association of Government Accountants, “Keep your boat afloat: Are you cybersecure?”
- Lipscomb Accounting Conference, “Auditing IT internal controls and IT security”
- Tennessee Electric Cooperative Association, “Utility Risk Management”
- IIA Nashville Chapter, “CAE Roundtable – Focus on Today: Implementing the Global Internal Audit Standards”
- Lipscomb Accounting Conference, TSCPA Chattanooga Chapter, “Soured Grapes: A Fraud Case Study in the Wine Industry”

SENIOR MANAGER

# Patrick Clark, CPA

*Patrick is a senior manager with Baker Tilly's risk advisory practice.*



**Baker Tilly Advisory Group, LP**

555 Great Circle Road
Nashville, TN 37228
United States

**T:** +1 (615) 921 5997
patrick.clark@bakertilly.com

**bakertilly.com**

## Education

Bachelor of Science in Finance and Accounting, Murray State University

Minimum 40 hours per year of continuing professional education

Patrick is responsible for planning and executing integrated internal audit engagements, evaluating effectiveness and efficiency of clients' business processes, building client relationships as well as preparing and presenting reports to management and boards of directors.

He primarily works with clients in the manufacturing, wholesale and distribution (MWD), utility and governmental industries. In addition to internal audit and risk management consulting, he has extensive experience assisting organizations in the design and implementation of Sarbanes-Oxley (SOX) compliance programs using the COSO 2013 Integrated Internal Controls Framework and leading the on-going testing, compliance and reporting. Patrick's internal audit and SOX experience includes assessments of entity level controls, general controls over information technology, fraud risk assessments and financial and operational business processes and controls.

Prior to joining Baker Tilly, Patrick had over 15 years combined experience serving as Vice-President of Internal Audit for a publicly traded global manufacturing company, and as Audit Director for a restaurant holding company with US and international operations, including both company-owned and franchised stores. As VP of Internal Audit, he was instrumental in implementing the company's first internal audit department, including establishing audit guidelines and approach, reporting, internal audit charter, hiring staff and formal communications to the Board and Audit Committee.

In both roles, he was responsible for managing the day-to-day activities of the internal audit department, preparing the annual risk assessment and audit plan, overseeing the SOX compliance programs, coordinating audit plans with the external auditors and communicating results with management and the Board.

Patrick has 30 years of professional accounting and internal audit experience, including as senior manager of business risk services at a Big Four firm.

## Industry involvement

- Institute of Internal Auditors, Past President–Nashville Chapter
- Friends of Nashville Opera, President 2023-2025; VP Strategic Development/Finance -2019-2023

SENIOR MANAGER

# Jamie Braswell, CIA

*Jamie is a senior manager with Baker Tilly's risk advisory financial services team.*



**Baker Tilly Advisory Group, LP**

555 Great Circle Road
Nashville, TN 37228
United States

**T:** +1 (615) 782 4227
jamie.braswell@bakertilly.com

**bakertilly.com**

## Education

Master of Business Administration
Tennessee Tech University

Bachelor of Science, Accounting
Tennessee Tech University

Jamie is a senior manager in the risk management services practice at Baker Tilly. She has more than 15 years of experience working with clients in multiple industries, including financial, manufacturing and wholesale/distribution, utility, governmental and others.

Jamie is primarily responsible for planning, performing and executing internal and external audits, risk assessments, Sarbanes-Oxley (SOX) program implementations, SOX controls testing and system and organization controls (SOC) attestation examinations, as well as enterprise risk management and other consulting engagements. In addition, Jamie regularly evaluates the effectiveness and efficiency of business processes, internal controls and risk management strategies. Specifically for financial institutions, she performs internal audits, loan reviews, National Automated Clearing House Association (NACHA) audits, trust department audits and compliance audits.

Jamie has successfully managed projects for several high-value clients in her career, including all aspects for a public financial institution with more than $50 billion in assets; outsourced integrated internal audit and consulting projects for the 11th-largest public utility in the United States; and for a private food manufacturer with more than $1 billion in annual revenue. She also has international work experience in China and Singapore, where she performed SOC engagements.

## Relevant examples of experience

- Led, oversaw and managed internal audit and assurance functions and teams for financial institutions of varying sizes and environments
- Provided leadership, oversight and expertise in a wide variety of areas including operations, financial, IT, SOX and specialized areas such as ACH, mortgage, loan review, trust and compliance for financial institutions
- Conducted NAHCA regulatory audits
- Consulted on strategic initiatives, regulatory compliance, industry best practices, internal controls, risk assessment and audit plan development

## Industry involvement

- Institute of Internal Auditors (IIA)

v

SENIOR MANAGER

# Alex Herrin, CPA, CISA

*Alex is a senior manager with Baker Tilly's risk advisory practice.*



**Baker Tilly Advisory Group, LP**

555 Great Circle Road
Nashville, TN 37228
United States

**T:** +1 (615) 921 6006
alex.herrin@bakertilly.com

**bakertilly.com**

## Education

Master of Accountancy
Bachelor of Science in accountancy
Mississippi State University

Alex is a senior manager with more than 10 years of experience and is responsible for coordinating, supervising and executing information technology (IT) internal audit services, network security and cybersecurity assessments and System and Organization Controls (SOC) attestation examinations, as well as evaluating the effectiveness and efficiency of business processes.

His experience includes IT audits, network and cybersecurity assessments, SOC readiness reviews and examinations for clients in a number of industries, including manufacturing, utilities, managed IT and information security. Additionally, he has experience with FFIEC IT regulatory audits and Sarbanes-Oxley (SOX) testing for financial institutions ranging from $1 billion in assets to approximately $42 billion in assets.

Prior to Baker Tilly, Alex was an information security analyst and IT internal auditor for a public regional bank with more than $12 billion in assets. As an information security analyst, Alex focused primarily on managing governance, risk, and compliance for the information security department. He also managed the phishing and event monitoring programs while interfacing with both internal and external audit to ensure successful regulatory and SOX audits. As an internal IT auditor, Alex led internal and SOX audits.

## Industry involvement

- American Institute of Certified Public Accountants
- Tennessee Society of Certified Public Accountants
- ISACA
- Institute of Internal Auditors
- Cloud Security Alliance

## Continuing professional education

- Certified Information Systems Auditor

**Recommendation for Approval of FY27 Internal Audit Plan, Audit & Ethics Committee Charter and Internal Audit Charter**

Internal Audit recommends approval of the FY27 Internal Audit Plan which includes 6,990 hours, the Audit & Ethics Committee Charter, and the Internal Audit Charter.

**Nashville Electric Service**
**Proposed 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 |
| Internal Control Framework Assistance | | 150 |
| ERM Assistance | | 375 |
| Follow-up and Remediation-Quarterly | | 250 |
| **Total FY27 Audit Plan Hours** | | **6,990** |

| | | |
|---|---|---|
| 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 |

**THE ELECTRIC POWER BOARD**
**OF THE METROPOLITAN GOVERNMENT**
**OF NASHVILLE AND DAVIDSON COUNTY**
**AUDIT & ETHICS COMMITTEE CHARTER**

## I. INTRODUCTION

The Audit Committee at Nashville Electric Service (NES) was established in October 1990 by the Electric Power Board (the "Board"). In August 1996, the Board made a decision to combine the Audit Committee and the Ethics Committee into one committee named the Audit & Ethics Committee. It represents the Board's commitment to maintaining management's accountability by providing independent oversight of the financial reporting and audit process. This independent committee directly influences the control environment. Through the Audit & Ethics Committee, the Board provides the ultimate level of public accountability and trust to NES 's customers.

## II. COMPOSITION AND ROLE OF THE AUDIT & ETHICS COMMITTEE

### A. COMPOSITION

The Audit & Ethics Committee consists of:

1. Two or more Board members and the Chair of the Board, who is an ex officio member, all of whom shall be independent.

2. The Vice President Chief Financial Officer shall serve as a non-voting ex officio member.

3. Board members on the Audit & Ethics Committee will be appointed by the Chair of the Board, and one will be designated to serve as the Committee Chair.

4. At least one member must meet the definition of a financial expert. This individual should possess the following skills: understands financial statements; can assess accounting for estimates, reserves, and accruals; has experience in preparing or analyzing financial statements; and understands internal controls.

### B. ROLE

1. The Audit & Ethics Committee's role is one of oversight, whereas management is responsible for the adequacy of the systems of internal control and procedures and for preparing the financial statements.

2. The Audit & Ethics Committee plays a key role in the integrity of the organization's financial reporting process and internal control structure, as well as the legal and ethical conduct of the organization's management and employees. The Audit & Ethics Committee shall:

a) Oversee the accounting and financial reporting processes and ensure effective and continuing internal and external independent audits and control procedures.

b) Ensure auditor independence.

c) Ensure that proper and timely attention is paid to control and compliance weaknesses.

## III. AUTHORITY AND RESPONSIBILITY OF THE AUDIT & ETHICS COMMI'ITEE

### A. AUTHORITY

1. Final decision-making authority is the responsibility of the full Board; therefore, the Audit & Ethics Committee will advise and make recommendations to the Board.

2. The Audit & Ethics Committee will advise management and the Outsourced Internal Audit Firm as their duties relate to financial accounting, reporting, internal controls, and compliance. In this manner, the Audit & Ethics Committee assists the Board in fulfilling its fiduciary responsibilities as to the accounting and reporting practices of NES, the adequacy of its auditing, and the adequacy of its disclosures to the public.

3. The Audit & Ethics Committee may cause special examinations or investigations to be conducted because of inefficiencies, improprieties, alleged illegal activities, and reports of impediments to the auditors.

4. The Chair of the Audit & Ethics Committee may have legal counsel present at any meeting or may seek legal counsel, accountants, or others to advise concerning the responsibilities and/or actions of the Committee.

### B. RESPONSIBILITY

1. The Audit & Ethics Committee is to serve as a focal point for communication between the Board members, the independent external auditors, the Outsourced Internal Audit Firm, and the organization's management as their duties relate to financial accounting, reporting, internal controls, and compliance.

2. The Audit & Ethics Committee should adhere to and enforce the Ethics Policy contained in the NES Policy Manual.

## IV. OPERATIONAL GUIDELINES

### A. AUDIT & ETHICS COMMITTEE MEETINGS

1. Meetings will be held at least four times a year and more frequently if the Audit & Ethics Committee deems it necessary.

2. The President & CEO and Vice President Chief Legal Officer & General Counsel may attend Audit & Ethics Committee meetings.

3. The Secretary of the Board will attend Audit & Ethics Committee meetings to perform the duties required by the Bylaws of the Board.

4. Other members of NES management may attend Audit & Ethics Committee meetings, as needed.

5. Representatives of the independent external auditors may attend Audit & Ethics Committee meetings.

6. The Audit & Ethics Committee may invite others to attend meetings; input may be sought from employees and/or the public if deemed beneficial.

7. The Audit & Ethics Committee may meet in executive session with the independent external auditors when they are present and/or with the Outsourced Internal Audit Firm. The Audit & Ethics Committee and the Outsourced Internal Audit Firm should meet at least annually without management present.

### B. AUDIT & ETHICS COMMITTEE MINUTES AND REPORTS

1. The Secretary of the Board will be responsible for calling meetings, filing reports, and recording minutes.

2. The Secretary will prepare the minutes of each meeting and obtain signed approval for the minutes from the Chair of the Audit & Ethics Committee.

3. The Secretary will forward a copy of the approved minutes to the other Board members.

4. The minutes will be formally approved at the next Audit & Ethics Committee meeting and recorded as such in those minutes.

5. Approved minutes will be made available for public inspection.

6. The Board will be apprised of significant developments through minutes or special presentations.

7. An update of significant items discussed in the Audit & Ethics Committee meetings will be presented to the Board following each Audit & Ethics Committee meeting.

## C. INDEPENDENT EXTERNAL AUDITORS

The Audit & Ethics Committee will:

1. Advise the Board as to the appointment and compensation of the external audit firm, including any non-audit services, and provide external auditor oversight. The Bylaws of the Board place some restrictions on non-audit services.

2. Review, prior to the annual audit, the scope and general extent of the external auditors' planned examination. The Audit & Ethics Committee should have an understanding from the external auditors of the factors to be considered in determining the audit scope, including:

    a) Risk characteristics of NES.

    b) External reporting requirements.

    c) Dollar amount and activities considered material.

    d) Quality of internal accounting, administrative, information technology, and compliance controls.

    e) Extent of the Outsourced Internal Audit Firm's involvement in the audit examination.

    f) Areas to be covered during the audit engagement.

3. Review with management and the external auditors' instances, if any, where management has obtained "second opinions" on accounting and financial reporting policies from other accountants.

4. Review with management and the external auditors, upon completion of their audit, financial statements for the year prior to their release to the public. The review should consider whether the financial statements are complete and consistent with information known to the Audit & Ethics Committee members and include discussion of:

    a) Significant accounting and reporting issues, including complex or unusual transactions and highly judgmental areas, recent professional and regulatory pronouncements, and the impact on the financial statements.

    b) Selection of and changes in accounting principles or their application, if any, during the year.

c) Significant adjustments proposed by the external auditors.

d) The process used by management in formulating accounting estimates and the external auditors' conclusion regarding the reasonableness of those estimates.

e) Any disagreements between the external auditors and management about matters which could significantly affect the financial statements or the auditors' report.

f) Difficulties encountered in performance of the audit.

g) The accuracy and completeness of other sections of the annual report.

5. Review with management and the external auditors all matters required to be communicated to the Committee under generally accepted auditing standards.

6. Review any reported recommendations the external auditors may have, management's written responses to the external auditors' recommendations for adequacy, and, if necessary, discuss with management the implementation of the recommendations along with completion dates.

7. Review the status of the implementation of prior-period recommendations and corrective action plans.

8. Make any necessary recommendations to the Board regarding the resolution of issues relative to the external audit.

9. Review the performance of the external auditors and make recommendations to the Board regarding appointment or discharge of the auditors.

10. Review and confirm the independence of the external auditors by obtaining statements from the auditors on relationships between the auditors and the organization, including non-audit services, and discussing the relationships with the auditors.

11. On a regular basis, meet separately with the external auditors to discuss any matters that the Audit & Ethics Committee or auditors believe should be discussed privately.

12. If the firm retains the contract for more than five years, consider whether the lead partner or lead member of the engagement team should rotate off of the audit.

## D. EXECUTIVE MANAGEMENT

The Audit & Ethics Committee will:

1. Consider the effectiveness of the organization's enterprise risk management program and internal control system, including information technology security and control.

2. Review the President & CEO and Vice President Chief Financial Officer's signed letter of representations addressed to the Audit & Ethics Committee certifying the appropriateness of the financial statements and disclosures contained in the annual report, and that those financial statements and disclosures fairly present, in all material respects, the operations and financial condition of NES.

## E. INTERNAL AUDIT

The Audit & Ethics Committee will:

1. Review and approve the Internal Audit Charter and consider amendments to the Charter, as may be required.

2. Review and approve the annual audit plan, including budgeted hours, prepared by the Outsourced Internal Audit Firm and any changes to the plan. The annual plan will include a tentative plan for two additional years. In evaluating the annual audit plan, the Audit & Ethics Committee may consider prior internal audit reports and heightened risk identified by enterprise risk management processes.

3. Review with management and the Outsourced Internal Audit Firm the activities of the internal audit function.

4. Advise the Board as to the appointment and compensation of the Outsourced Internal Audit Firm and review and approve any contractual adjustments.

5. Review internal audit reports and management responses and, if necessary, discuss with management the implementation of the recommendations along with completion dates.

6. Ensure there are no unjustified restrictions or limitations, and review and concur in the appointment, replacement, or dismissal of the Outsourced Internal Audit Firm.

7. At least once per year, evaluate the performance of the Outsourced Internal Audit Firm.

8. At least once per year, receive and review confirmation of the Outsourced Internal Audit Firm's organizational independence. This includes communicating incidents where independence may have been impaired, and the actions or safeguards employed to address any impairment.

9. Review the effectiveness of the internal audit function and determine whether the Outsourced Internal Audit Firm has reviewed the reliability and integrity of financial and operating information and examined compliance with regulations, laws, policies, and the internal systems in place to assure compliance.

10. Review compliance with The Institute of Internal Auditors' mandatory elements of the International Professional Practices Framework, which are the Global Internal Audit Standards and Topical Requirements, including the principles of Ethics and Professionalism,

11. Review compliance with the Government Accountability Office (GAO) Government Auditing Standards.

12. On a regular basis, meet separately with the Outsourced Internal Audit Firm to discuss any matters that the Committee or the Outsourced Internal Audit Firm believes should be discussed privately, including anonymous Integrity Line submissions of concerns by employees.

## F. COMPLIANCE

The Audit & Ethics Committee will:

1. Review the effectiveness of the system for monitoring compliance with laws and regulations and the results of management's investigation and follow-up of any instances of non-compliance.

2. Review the findings of any examinations by regulatory agencies and any auditor observations.

3. Obtain regular updates from management and legal counsel regarding compliance matters.

4. Review the process for monitoring conflicts of interest.

## G. AMENDMENTS

Any recommended modification or amendment to this Charter must be included on the official Audit & Ethics Committee meeting agenda, and a draft of the modification or amendment must be provided to the members of the Committee in advance. The Audit & Ethics Committee may modify or amend this Charter by an affirmative vote of a majority of its members. Amendments or modifications approved by the Audit & Ethics Committee will be submitted to the Board for final approval.

## H. MISCELLANEOUS

The Audit & Ethics Committee may:

1. Perform other activities related to this Charter as requested by the Board and appeal to the Board issues which it cannot resolve.

2. Recommend any appropriate extensions or changes m the duties of the Committee to the Board for approval.

3. Review and assess the adequacy of the Committee Charter annually and request Board approval for proposed changes.

4. Confirm annually that all responsibilities outlined in this Charter have been carried out.

5. Evaluate the Committee's and individual members' performance on a regular basis.

Approved this 22nd day, July 2026

_____
Chair of the Electric Power Board

_____
Chair of the Audit & Ethics Committee

*Approved as to Form and Legality:*

_____
VP Chief Legal Officer & General Counsel

*Outsourced Internal Audit Firm:*

_____
Baker Tilly Advisory Group, LP

**NASHVILLE ELECTRIC SERVICE**
**INTERNAL AUDIT CHARTER**

## I. MISSION AND SCOPE OF WORK

The mission of NES Internal Audit Outsourcing is to provide independent, objective assurance and consulting services designed to add value and improve the organization's operations. Internal Audit assists the organization in accomplishing its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance processes.

The scope of work of the Outsourced Internal Audit Firm is to determine whether the NES risk management, control, and governance processes, as designed and implemented by management, are adequate and functioning in a manner to ensure:

- Risks are appropriately identified and managed.
- Significant financial, managerial, and operating information is accurate, reliable, and timely.
- Actions comply with policies, procedures, and applicable laws and regulations.
- Assets are acquired economically, used efficiently, and adequately protected.

The Outsourced Internal Audit Firm will adhere to the mandatory elements of the Institute of Internal Auditors' International Professional Practices Framework, which are the Global Internal Audit Standards and Topical Requirements, including the principles of Ethics and Professionalism. The Outsourced Internal Audit Firm will report periodically to the Electric Power Board through the Audit & Ethics Committee and NES senior management regarding the Internal Audit Function’s conformance to the Standards, which will be assessed through a quality assurance and improvement program. In addition, the internal audit activity will adhere to Government Accountability Office (GAO) Government Auditing Standards, relevant NES policies and procedures, and the internal audit activity's standard operating procedures manual.

## II. ACCOUNTABILITY

The Outsourced Internal Audit Firm shall be functionally accountable to the Electric Power Board through the Audit & Ethics Committee with administrative oversight provided by the President & CEO to:

- Provide an assessment of the adequacy and effectiveness of the organization's processes for controlling its activities and managing its risks in the areas set forth under the mission and scope of work.

- Report significant issues related to the processes for controlling the activities of NES, including potential improvements to those processes.

- Provide information periodically on the status and results of the annual audit plan.

- Coordinate with the external auditors, Legal, Utility Compliance, Environmental Compliance Group, and Security, as appropriate.

## III. INDEPENDENCE AND OBJECTIVITY

The Outsourced Internal Audit Firm reports to the Audit & Ethics Committee of the Electric Power Board and will annually confirm the organizational independence of the internal audit activity. This includes communicating incidents where independence may have been impaired, and the actions or safeguards employed to address any impairment.

The Audit & Ethics Committee is responsible for the evaluation, appointment, or removal of the Outsourced Internal Audit Firm. The Outsourced Internal Audit Firm will communicate and interact directly with the Electric Power Board, through the Audit & Ethics Committee, including in executive sessions and between meetings, as appropriate. The Audit & Ethics Committee will make appropriate inquiries to determine whether there is inappropriate scope or resource limitations.

The internal audit activity will remain free from interference by any element in the organization, including matters of audit selection, scope, procedures, frequency, timing, or report content to permit maintenance of a necessary independent and objective mental attitude.

Internal auditors will exhibit the highest level of professional integrity, objectivity, and confidentiality in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors will make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments.

Internal auditors will have no direct operational responsibility or authority over any of the activities they review. Accordingly, internal auditors will not implement internal controls, develop procedures, install systems, or engage in other activities that may impair their judgment.

Internal auditors will disclose impairments of independence or objectivity, in fact or appearance, to appropriate parties and at least annually, such as the Internal Audit Director, Board, and management.

## RESPONSIBILITY

The Outsourced Internal Audit Firm is responsible for:

- Developing an annual audit plan using risk-based methodology, including any risks or control concerns identified by management, and submitting that plan to the Audit and Ethics Committee for review and approval. The audit plan will consist of a work schedule as well as budget and resource requirements.

- Implementing the approved audit plan, including, as appropriate, special projects requested by management or the Audit & Ethics Committee.

- Maintaining an Internal Audit Function that collectively possesses the knowledge, skills, experience, and professional certifications to meet the requirements of this Charter and the Global Internal Audit Standards.

- Establishing a review process by which the Outsourced Internal Audit Firm assures the effectiveness of the operation of internal auditing activities.

- Performing facilitation, process design, or training at management's request to assist management in meeting its objectives.

- Evaluating and assessing new or changing processes and control activities coincident with their development or implementation.

- Issuing periodic reports to management and the Audit & Ethics Committee summarizing results of audit activities.

- Following up on findings and recommendations and maintaining an open issues file until cleared.

- Performing periodic analyses of the audit plan versus emerging or changing risks and communicating any significant deviations from the approved plan.

- Reporting periodically on the internal audit activity's purpose, authority, and responsibility.

- Performing consulting and advisory services related to governance, risk management and control as determined appropriate.

- Keeping management and the Audit & Ethics Committee informed of emerging trends and successful practices in internal auditing.

- Providing measurement goals and results to the President & CEO.

- Assisting in the investigation of significant suspected fraudulent activities within the organization and notifying management and the Audit & Ethics Committee of the results.

- Reviewing and assessing the adequacy of the Internal Audit Charter annually and requesting Audit & Ethics Committee approval for proposed changes.

- Facilitating and reporting the results of the annual Enterprise Risk Management (ERM) process performed by NES Management to the Audit & Ethics Committee. Internal Audit is not responsible for developing or implementing any of the mitigating controls identified by NES Management.

The Outsourced Internal Audit Firm is not authorized to:

- Perform any operational duties for the organization, including, but not limited to, implementing internal controls, developing procedures, installing systems, preparing records, or engaging in any activity that may impair internal auditor's judgment.

- Initiate or approve accounting transactions.

- Direct the activities of any employee.

## IV. AUTHORITY

In carrying out the internal audit objectives, the Outsourced Internal Audit Firm is authorized to:

- Have access to all of NES's functions, records, properties, and personnel. This authority extends to third-party processors and independent contractors.

- Have access to the Audit & Ethics Committee.

- Allocate resources, set frequencies, select subjects, determine scopes of work, and apply the techniques required to accomplish audit objectives.

## V. QUALITY ASSURANCE AND IMPROVEMENT PROGRAM

The internal audit activity will maintain a quality assurance and improvement program that covers all aspects of the internal audit activity. The program will include an evaluation of the internal audit activity's conformance with the Global Internal Audit Standards, as well as performance measurement to assess the internal audit function’s progress toward the achievement of its objectives and promotion of continuous improvement, and conformance with GAO Government Auditing Standards. This program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement.

The Outsourced Internal Audit Firm will communicate to executive management and the Electric Power Board on the internal audit activity's quality assurance and improvement program, including results of ongoing internal assessments and external assessments conducted at least every three years.

## VI. AMENDMENTS

Any recommended modification or amendment to this Charter must be included on the official Audit & Ethics Committee meeting agenda, and a draft of the modification or amendment must be provided to the members of the Committee in advance. The Audit & Ethics Committee may modify or amend this Charter by an affirmative vote of a majority of its members. Amendments or modifications approved by the Audit & Ethics Committee will be submitted to the Electric Power Board for final approval.

Approved this 22nd day, July 2026

_____
Chair of the Electric Power Board

_____
Chair of the Audit & Ethics Committee

*Approved as to Form and Legality:*

_____
VP Chief Legal Officer & General Counsel

*Outsourced Internal Audit Firm:*

_____
Baker Tilly Advisory Group, LP

Executive Session