OFFICE OF INTERNAL AUDIT AND ETHICS

738 Acquoni Road
PO Box 455
Cherokee, NC 28719

p. (828) 359-7030
w. oia.ebci-nsn.gov
e. oia@ebci-nsn.gov

June 9, 2026

Executive Office
Tribal Council
The Eastern Band of Cherokee Indians
Cherokee, NC

We conducted an Information Technology Governance audit in accordance with the FY26 annual audit plan.

An information technology governance audit is designed to assess the Tribal-wide IT operations and effectiveness of internal controls to determine if improvement is needed.

Protiviti identified 1 observation. The details can be found in the attached report. Management's action plan is included as an attachment.

The assistance of the Information Technology staff is appreciated. Please do not hesitate to contact our office with questions.

Sincerely,

Sharon Blankenship, CIA, CGAP, IAP, CFE, LPEC
Chief Audit and Ethics Executive

cc: Monique Taylor, Audit and Ethics Committee Chair
Paxton Myers, Chief of Staff
Kevin Jackson, Information Technology Director

IT Change Management
Internal Audit Report

May 2026

protiviti®
Face the Future with Confidence

Table of Contents

***Disclaimer**: This report provides management with information about the condition of risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel will impact these risks and internal controls in ways this report cannot anticipate. This document is intended for management use and should not be relied upon by any third party.*

Background

IT governance supports the alignment of information technology activities and organizational objectives, while providing oversight of IT risks, security, investment decisions, and performance. Effective IT governance establishes clear decision-making authority, defined oversight practices, and consistent processes across strategy, value delivery, risk management, information security, and performance monitoring, reducing the risk of misalignment, unmanaged risk, or ineffective use of IT resources.

The Eastern Band of Cherokee Indians performs key IT governance activities through a combination of ad hoc practices based on organizational policy, management oversight, and operational processes. These activities include IT strategy and project prioritization, oversight of major IT initiatives, management of IT risks and security, cyber incident preparedness, and periodic reporting of IT performance and risks to leadership.

The IT Governance program was selected for review as part of the 2026 Internal Audit annual plan. Internal Audit assessed IT governance practices, focusing on whether key governance processes are formally defined, consistently performed, and supported by appropriate documentation and management oversight across strategy, risk, security, and performance monitoring domains.

Scope & Objectives

The audit was designed to identify and evaluate the internal controls related to these IT Governance themes, including:

- **Strategic Alignment:** Controls over the alignment of IT strategy to overall Tribal goals, IT organization roles and responsibilities, project intake and prioritization processes and governance forums.
- **Governance Structure & Oversight:** Controls to ensure proper leadership and oversight practices and efficient IT reporting and monitoring related to IT strategic goals
- **Risk Management & Compliance:** Controls to identify and define key IT risks are documented, IT security policies exist and are regularly reviewed and updated, and best practices in the event of a cybersecurity incident are followed.
- **Value Delivery & Performance:** Controls to ensure all major IT projects are properly proposed, reviewed and approved, documentation around these key projects is stored in a centralized repository are in place. Controls to ensure IT service metrics and SLAs are properly reviewed, and issues are tracked, escalated and resolved are in place.
- **Performance Measurement & Continuous Improvement**: Controls to ensure IT performance metrics and trends are reviewed to identify improvement opportunities and inform future planning and governance activities.

Summary of Audit Procedures

Internal Audit’s approach included:

- Conducting interviews to walk through and gain an understanding of governance processes.
- Conducting testing procedures over identified control activities.
- Identifying potential areas for risk mitigation and control design improvement.

High-Level Conclusions & Observations Count by Risk Ranking:

The audit identified the finding summarized below. Additional details, including remediation recommendations, can be located within the "Detailed Observations" section of this audit report.

1. **IT Governance Framework :** Internal Audit determined that EBCI's IT governance practices are largely informal, decentralized, and inconsistently executed. Performance monitoring and risk visibility are limited due to the absence of standardized metrics, reporting, and documentation. Without a formal governance framework, defined roles, and documented oversight, day-to-day decisions rely on individual judgment, reducing consistency, accountability, and sustainability.

High (0)	Moderate (1)	Low (0)	Total (2)

Risk Definition and Classification Process

As you review each observation within the Detailed Observations and Action Plans Matrix of this report, please note that we have included a color-coded depiction as to the perceived degree of risk represented by each of the observations identified during our review. The following chart provides information with respect to the applicable definitions and terms utilized as part of our risk ranking process:

	Degree of Risk and Priority of Action	
Risk Definition - The degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management.	High	The degree of risk is unacceptable and either does or could pose a significant level of exposure to the organization. As such, immediate action is required by management in order to address the noted concern.
	Moderate	The degree of risk is undesirable and either does or could pose a moderate level of exposure to the organization. As such, action is needed by management in order to address the noted concern and reduce risks to a more desirable level.
	Low	The degree of risk appears reasonable; however, opportunities exist to further reduce risks through improvement of existing policies, procedures, and/or operations. As such, action should be taken by management to address the noted concern.

It is important to note that considerable professional judgment is required in determining the overall ratings presented on the subsequent pages of this report. Accordingly, others could evaluate the results differently and derive different conclusions.

It is also important to note that this report provides management with information about the condition of risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.

Detailed Findings

Observation Category	Detailed Observation	Risk Description	Risk Rating
1. IT Governance Framework	Through testing of key governance controls based upon the five thematical areas identified in the Scope & Objectives section above, Internal Audit identified that IT governance activities at EBCI are largely performed through informal, ad hoc, and decentralized practices rather than through a formally defined and consistently executed IT governance framework. Additionally, performance monitoring and risk visibility are inconsistent due to the lack of standardized metrics, reporting, and documentation. While management oversight, discussions, and operational decision-making occur in practice, the absence of a formal IT governance charter, clearly defined governance roles and forums, standardized processes, and documented oversight mechanisms limits sustainability, transparency, accountability, and scalability of IT governance as the organization and technology environment evolve. Without a formalized IT governance model, EBCI remains reliant on individual knowledge and management discretion rather than institutionalized controls, increasing the risk that governance practices will be inconsistently applied, difficult to evidence, and less effective over time.	The absence of a formalized IT governance framework increases the risk of inconsistent control execution, limited transparency and accountability, reduced ability to evidence oversight, and diminished effectiveness and scalability of governance as organizational and technology complexity grows.	Moderate

Observation Category	Detailed Observation	Risk Description	Risk Rating

Recommendation:

Internal Audit recommends that EBCI establish a *formal, lightweight IT Governance framework* commensurate with its risk profile, including:

- A formal IT Governance Charter defining governance intent, scope, decision-making authority, roles, and responsibilities.
- A formal governance cadence for oversight of strategy, reviewing goals and updating policy and procedures.
- Standardized project intake, prioritization, and performance monitoring mechanisms.
- Defined KPIs, risk registers, and reporting processes to support consistent oversight and continuous improvement.

This approach would formalize existing practices, improve accountability and visibility, and support sustainable IT governance without introducing unnecessary operational complexity.

OFFICE OF INTERNAL AUDIT AND ETHICS

738 Acquoni Road
PO Box 455
Cherokee, NC 28719

p. (828) 359-7030
w. oia.ebci-nsn.gov
e. oia@ebci-nsn.gov

MEMORANDUM

TO: Executive
Tribal Council

FROM: Sharon Blankenship, Chief Audit and Ethics Executive

CC: Monique Taylor, Audit and Ethics Committee Chair
Paxton Myers, Chief of Staff
Kevin Jackson, IT Director

DATE: June 9, 2026

RE: Action plan for 26-005 – Information Technology Governance

The observation and recommendation identified in the Information Technology Governance audit report 26-005 was sent to the program for an action plan. The action plan as provided is stated below. The original response forms are on file with this office.

1. IT Governance Framework

Response: Agree, Target implementation 9/1/26

Respondent narrative: " **Phase 1** A. Develop the following: IT Governance Charter Consisting of the following: Purpose, Authority, Membership, Roles & Responsibilities, Decision making authority, Meeting schedule, Reporting requirements, Alignment with Tribal strategic goals, Data sovereignty principles, B. Governance Committee w/quarterly meetings, **Phase 2** Formalize Project Governance, create Project intake process and prioritization Matrix, **Phase 3** Implement IT Risk Governance, **Phase 4** Develop KPI Dashboard around all programs of the OIT Division."