North Carolina Community College System Office

2026-2027 Risk Assessment and Internal Audit Plan

Annual Risk Assessment Process

The internal audit risk assessment is an annual and on-going risk-based exercise established to identify concerns and potential risk areas to be considered for inclusion in the annual audit plan and as a source of agency wide risk intelligence gathering. It is relied upon by senior management as an independent perspective on potential areas of agency risk.

Risks identified are grouped where relevant and ranked based on the likelihood and impact of the risks. Risks are then ordered by overall rating and communicated to management. Management and Internal Audit discuss the risk priorities to determine which items would be best addressed through audit or consultation, and which items will be managed by management. The higher risk areas, along with how these areas are being addressed by Internal Audit, are shown on the table below:

Risk	Audit Plan or response
VERY-HIGH RISK AREAS	
ERP: Challenges of implementing a new ERP system: Incomplete installation of ERP, issues to critical systems during development, reduced services to students, loss of faith in systems from students and college staff.	Not on plan. Due to the high level of governance and resource constraint. Other areas have a higher audit value.
Cybersecurity: These risks include an evolving risk landscape and variety of potential events.	**On the current audit plan, 240 Hours.**
Record Retention: There is a large volume of paper records in the building. These records are not backed up. Loss of records risk.	Recently Audited. Completed in FY 25-26
HIGH RISK AREAS	
Risk Management: Risk Management processes are not formalized. Risk identification and mitigation are not documented.	**On the current audit plan, 240 hours.**
Grant Management: Noncompliance with Grants may occur as the process for grant management is decentralized and left up to each Grant Manager.	**On the current audit plan, 180 hours**
SOPs: Non-existent or outdated Policies and SOPs. Communications of SOPs, tracking SOPs.	Recently Audited. Completed in FY 25-26
Human Resources Risk Areas: Turnover in key leadership positions. Inconsistent priorities reduce effectiveness. The System Office operates with a very lean staff. Initiatives are increasing, overall headcount does not match the demands.	Not on the audit plan due to resource constraints. This will be tracked for future audits.
PropelNC: Implementation of PropelNC, failure for the program to achieve desired changes in program outcomes.	Not on the plan. Too soon for an audit.
Contract Management: Vendor management, third party risk management.	**On the current audit plan, 180 hours.**
MEDIUM RISK AREAS	
IT Systems: Legacy systems, system maintenance, outdated technology, matching skills to evolving systems, systems access, etc.…	Possible contract in FY 26-27 due to specific skill requirements and resource limitations.
Legislative Risks/ Federal Funding Risks: Risk of budgetary restrictions, risk of increased regulatory requirements.	Outside of system office control, not an auditable area.
Marketing: Inconsistent marketing and outreach, lack of formal processes to identify and reach business partners for economic development, inconsistent marketing of added value and being a "well-kept secret".	Not on the audit plan due to resource constraints. This will be tracked for future audits.
Governance and Culture: Poor culture and low morale impact turnover and effectiveness.	Not on the audit plan due to resource constraints. This will be tracked for future audits.
I-9 Compliance: Many audit shops consider this an emerging risk area with heavy fines for compliance issues.	**On the current audit plan, to be performed by interns. 40 Hours.**

The determination of which areas to audit and which areas to continue to monitor and consider for future audits is based on the resources available for internal audit. While the Internal Audit function is limited to one person, the function has been pursuing the use of interns and contractors to help increase the amount of coverage that the function can provide.

Allocation of Available Hours for FY 2026-2027 (July 2026 – June 2027)

Available Hours of 1 FTE	2,080 hours
Administration (Meetings, CPE, PTO)	572 hours (28%)
Engagements	1,508 hours (78%)

Engagement Hours:

- Risk-Based Engagements (see below) 880 Hours (58% of engagement hours)
  - Cybersecurity 240 hours
  - Risk Management 240 Hours
  - Grant Compliance 180 Hours
  - Contract Management 180 Hours
  - I-9 Compliance (performed by interns) 40 Hours
- Other Engagements 100 Hours (7% 0f engagement hours)
  - Office of State Audit 2023 IT audit follow-up
- Other Required Activities 538 Hours (35% of engagement hours)
  - Annual Required Projects (SAMM, EAGLE, Council items) 234 hours (16%)
  - Statutory (Internal Audit Act: QAR, Process improvement) 88 hours (7%)
  - Recurring Engagements (Risk Assessment, Follow up) 166 hours (11%)
  - Placeholder hours 40 hours (3%)

July 2026- June 2027 Audit Plan: Pending Approval

Engagement	***Focus area / Preliminary Objective***	***Risk Rating***
Risk Based Engagements		
Cybersecurity	Compliance Audit regarding execution of control processes.	Very High
Risk Management Consulting Engagement	Consulting engagement to automate management risk register, document ERM processes.	High
Grant Management	Audit of processes to ensure compliance with grant requirements, including reporting and expenditures.	High
Contract Administration Audit	Audit of controls to manage contracted vendors and ensure deliverables are received.	Medium
Compliance Audits	I-9 compliance (intern support).	Medium
Other Engagement		
2023 OSA IT Audit Follow up	Determine the status of implementing processes developed as a result of the 2023 Information Systems Audit conducted by the Office of the State Auditor (OSA).	N/A