Greenville
TECHNICAL COLLEGE

Audit Committee
Meeting Minutes

November 20, 2024, at 11:00 a.m.
Student Success Center, Room 226

Members Present	Members Absent	Staff Present
Paul Batson		George Abraham
Tom Britt		Jacqueline DiMaggio
Hunter Howard, Chair		Julie Eddy
Ray Lattimore		Artie Hammond
Kenneth Southerlin		Lisa Mangione
		Keith Miller
		Lauren Simer

Call to Order

Chair Hunter Howard called the Audit Committee meeting to order at 11:00 a.m. and welcomed committee members, guests, and staff.

Approval of Minutes

Chair Howard requested a motion to approve the September 18, 2024, minutes as distributed. Mr. Paul Batson made the motion; Chair Howard seconded; the motion carried.

Risk Assessment Plan 2025

Mr. Artie Hammond presented a 2025 Internal Audit Plan handout and gave a brief overview of its development. His team keeps abreast of current risk trends in higher education, follows best practice guidelines from the Association of College and University Auditors, and conducts an annual assessment questionnaire of the college's management team of 30 auditable areas. The questionnaire included eight common risk factors and provided the opportunity to identify potential risks/concerns. Based on feedback from the questions, the risk/concerns are rated on a scale of "Potential Impact" times "Likelihood" and given a total "Risk Rank" score. These areas are then ranked high to low based on the given score. The top five areas identified based on the Risk Rank score were Financial Aid (FA), Office of Information Technology (OIT), Payroll, Human Resources (HR), and Learning and Workforce Development (LWD). FA is heavily audited every year; OIT was recently addressed in the Cybersecurity Assessment and Review; since the college is implementing a new ERP system, plans are to wait until after the implementation to test procedures and controls of HR and Payroll; LWD is in the Plan as an ongoing audit item.

The 2025 Plan contains two carry-over audits plus an additional special request from the 2024 Plan due to significant resources devoted to several special audits during the year. The 2025 Plan also contains the required compliance annual audits and FA. Lastly, the 2025 Plan comes from the department-specific risks and concerns questionnaire—GT Foundation (Foundation-funded credit card and reconciliation process); Student Affairs/FA (intake process interfacing with FA).

The college was asked how fixed assets were audited, and Ms. DiMaggio informed the committee that the state requires the college to scan 100% of fixed assets annually. For missing items, the college investigates whether the item was relocated from its original location and the records need to be updated, or if it is not located, the college must file a police report. Historically, the number of missing assets yearly has been minimal; however, this will be added to the audit list.

Chair Howard requested a motion to adopt the Plan as presented; Mr. Batson made the motion; Mr. Tom Britt seconded; the motion carried.

Initial Cybersecurity Plan

Mr. George Abraham reviewed the college's cybersecurity directives developed following CISA, an agency of the US Government that oversees information security policies and practices. The directives are a living document to be reviewed and tested frequently, so most will live in an ongoing state. Greenville Technical College does have a qualified individual tasked to oversee the college's cybersecurity program, and the college has successfully enforced multi-factor authentication (MFA) across all platforms. Currently, MFA is the college's best line of defense against unauthorized access. With the implementation of the new ERP system, some in-house applications will migrate to a Microsoft-based power platform, thereby creating a more secure environment.

Mr. Abraham noted that the college receives phishing emails and text messages impersonating colleagues and managers and has seen a considerable uplift in student phishing scams and transcript and application fraud. Faculty, staff, and students are often reminded to be vigilant before clicking links or opening attachments from suspicious sources, and annual IT security training is required for all employees. He reported that the college recently came under attack by BOTS, which denied outside services; however, the college was able to move one of its DNS servers to a third-party system, CloudFlare, within two hours, mitigating the disruption of services.

New, third-party products the college recently purchased, anticipated purchases to be made over the next calendar year, and products to be decommissioned were discussed, plus plans to develop a third-party solutions document for all IT-related bids and contracts as well as laying the groundwork for the college's Data Governance Council.

Cybersecurity insurance coverage, deductibles, and premiums were also discussed. Currently, the college has $5,000,000 coverage, $50,000 deductible, and approximately $70,000 premium.

The disaster recovery plan is currently being updated and will be discussed at a later meeting.

Old and New Business

There was no other business before the committee, so Chair Howard adjourned the meeting at 11:43 a.m.