The Audit, Risk, and Compliance Committee held its regular quarterly meeting on July 19, 2018. Chair Michael Drummond called the meeting to order and read the required ethics statement. Members of the committee in attendance were: Ms. Daniels, Ms. Kidd, and Ms. Beane.

The meeting began with the review and approval of minutes from the meeting that occurred on April 19, 2018.

The Audit, Risk and Compliance Committee updates began with Ms. Sharyne Miller, our Chief Information Officer, presenting recent UNC System Office Policy changes. She began with an overview of recently approved UNC Board of Governors’ IT policies that now necessitate that UNCW’s IT governance framework and policies be updated.

However, after a brief discussion and at the request of the Chancellor, the Committee tabled the action items as presented. This will be discussed at a later meeting, possibly prior to the October Audit, Risk, and Compliance Committee.

Mr. Corby Johnson then presented the Office of Internal Audit’s annual audit plan, or work plan. He explained the process used to develop the audit plan, and the items included on the plan. After the overview and a brief discussion, the Audit, Risk, and Compliance Committee approved the audit plan.

Mr. Johnson next presented Internal Audit’s activity report. He provided a high level overview of the work completed during the quarter ending June 30, 2018, and an overview of current and upcoming projects.
Mr. Johnson concluded his report by discussing the Facilities – Project Management audit that was completed and sent to members of the committee on July 16, 2018.

Ms. Sharon Boyd was our last presenter, and she provided an update on institutional risk management activities. The focus of the presentation was on UNCW’s mitigations related to the Tier I risks. These risks currently include:

- attracting and retaining high quality, diverse faculty and staff
- enrollment: attracting and retaining high quality student populations
- deferred maintenance and swing space for specialized facilities
- information security (breach and service interruption)
- revenue sufficiency to meet strategic goals
- community engagement (i.e., minors)