Assessment:

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. At the beginning of the module, attendees will asked as group to enumerate as cyber security first principles in general. At the end of the module attendees will be asked to again enumerate the cyber security principles, only this time emphasizing the relation to database systems. Both times this will be performed orally as a group. Experiments with database queries a means to explore use of basic operation systems commands on different platforms, and applying knowledge gained in solving real-world, scenario-based problems. Experiments with the vulnerable database system will realize the importance of secure coding and need for effective programming techniques to improve security A few pre/post camp questions will provide a degree of formal assessment.

Suitability to various groups:

The contents the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how the database systems can be integrated into the K-12 curriculum with emphasis on securing information stored in databases. The contents will also advance in the level of detail when being presented to the high school group compared to content being presented to the middle school students.

How the Teachers and Students groups will be interacting:

This module will not have explicit interaction amongst the three groups. Contents covered in the teachers group will primarily focus of how to integrating these security concepts in the K-12 curriculum, while those to students will focus on kindling their interest in the area of cybersecurity. Also, input from the teachers will be sought on how to better deliver the module contents to the other two students groups.