Overall Description of the Organization, IT Department, and Scope

University **ITMM IT Audit** ("the University") is situated on the southern coast of Florida (FL). The University offers associate, baccalaureate, masters, and/or doctoral degrees in arts, humanities, natural and social sciences, as well as in professional areas such as business, education, nursing, law, and medical technology. Currently, there are approximately 15,000 students attending the University.

In regards to IT and related support activities, the University's approach is centralized. That is, the University's computer processing is performed by the IT department, which is the sole provider of technology and telecommunications for the University's departments. Furthermore, the IT department provides data processing and end-user support for the University's systems and applications, including training and documentation of application system controls and procedures. The IT department's organizational structure consists of 30 staff, under the direction of an IT Executive Director.

The scope of this risk assessment is the University's financial application system. The application is called Banner Finance ("Banner") and runs on a Red Hat Enterprise Linux operating system. Refer to Exhibit A1.

Collection of Information Relevant for the Risk Assessment

During the risk assessment process, relevant information is gathered via reviews and inspections of documentation, as well as on-site interviews with key management personnel. Key management personnel for purposes of this example include:

- IT Executive Director (ITED)
- Banner Security Administrator (BSA)
- Operations Supervisor (OS)
- Systems Administrator (SA)
- Network Administrator (NA)

When interviewing the ITED and the BSA, it was noted that Banner holds critical and sensitive information about finance, accounting, human resources (HR), and payroll. The BSA further added that users of Banner include finance, accounting, HR, and technical/IT support personnel. Based on review of documentation, the University has several policies and procedures in place related to information systems operations, information security, and change control management.

In regards to the network infrastructure, the NA indicated that the University provides a wide variety of networking resources to all qualified members within the university community. Access to computers, systems, and networks is a privilege which imposes certain responsibilities and obligations, and which is granted subject to university policies, as well as local, state, and federal laws. All users must comply with policies and guidelines, and act responsibly while using network resources.

Physical access to the University's facilities and its data center, according to the ITED and the OS, is restricted through security mechanisms, including (1) biometric devices, (2) security guards, (3) video surveillance, and (4) visitors' logs. The authority to change the above physical access control mechanisms is limited to the ITED. The OS also stated that the University has implemented various environmental controls in order to prevent damage to computer equipment, and to protect data availability, integrity, and confidentiality. They are as follows: fire suppression equipment (i.e., FM-200 and fire extinguishers), uninterruptible power supplies, alternate power generators, and raised floors.

When asked about logical information security around Banner both, the SA and BSA, agreed on the following:

- Some password settings have been configured although current configuration is not consistent with industry best practices.
- Reviews of user access within Banner are conducted, but not on a periodic basis. Terminated user accounts are removed from Banner, but not in a timely manner. Documentation supporting reviews and removal of user access is not maintained.
- Programmers are restricted to work changes and modifications (i.e., updates and upgrades) to Banner in a test/development environment prior to their implementation in production. However, test results are not reviewed by management (i.e., ITED) nor approved before final implementation in production.

Lastly, Banner information is backed up daily though the OS stated that such daily backup is stored locally as the University has no offsite facility in place for backup storage.

This being the first such risk assessment, there are no previously generated documentation for the risk assessment team to review.