The Division of Information Technology
University Information Security Standards

Information Security Standard – Risk Assessment Reviews (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

The purpose of this standard is to implement a monitoring process which adequately provides management with assurance that the information on which risk assessment assertions are made is correct. The goal of these procedures is to assist West Texas A&M University departments with improving the effectiveness of their use of the risk assessment system and the value and accuracy of their information security risk assessments.

Information security risk assessments are vital procedures for maintaining the security of information resources and meeting legal requirements for protecting confidential information. The purpose and goal of these assessments can only be achieved if the assessments are conducted effectively.

2. Applicability

This standard applies to all information security risk assessments of information resources that are attached to the West Texas A&M University network. The intended audience includes all university personnel involved in performing, approving, or making risk management decisions related to information security risk assessments.

3. Definitions

3.2 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures,

equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3.1 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

3.3 Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

3.3 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

4. Procedures

4.1 The information security officer (ISO) will schedule meetings with appropriate personnel from West Texas A&M University departments to review their departmental information security risk assessment(s). After completion of the annual risk assessments, all of the departmental assessment reports will receive an internal review (Level 1). Based on the internal review, some departments will be selected for a more in depth review (Level 2). The selection of departments for a Level 2 review and the order of these reviews will be predicated on areas on inherent risk (e.g. confidential information, mission critical systems, and problematic conditions) or at the direction of the Chief Information Officer.

4.2 Each department selected for a Level 2 review will receive an email describing a general outline of the review process prior to the meeting. Departments will provide the ISO with requested information and assistance for the review. This may include assistance in performing an analysis of the department's information resources. Where beneficial and feasible, these reviews may utilize automated software tools to provide confirmation and/or information regarding the configuration and classification (e.g. contains confidential information and/or mission critical data) of the department's information resources. Such a process will be conducted efficiently and in a reasonable period of time.

4.3 The information security officer (ISO) will answer any questions departmental personnel have regarding the risk assessment process with the goal of promoting a better understanding and effective use of the risk assessment process. The ISO will seek suggestions that would benefit the department regarding clarifying and improving the risk assessment tool(s) and process.

4.4 Upon completion and analysis of the review, the information security officer (ISO) will provide a draft report to the division/department head or director and to any departmental personnel designated by the division/department head or director. After the draft report is delivered to the division/department head or director, there will be an approximately two week period for discussion and any appropriate modifications to the report. The final report will be provided to the Chief Information Officer or designee, the division/department or director, and designated departmental personnel within approximately three weeks of the conclusion of the review.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer