Texas A&M University System Standard – Information Security Risk Assessment Reviews

Standard Statement

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 standards is to assist the System Office (SO) with improving the effectiveness of its use of the risk management system and the value and accuracy of their information security risk assessments.

Reason

Information security risk assessments are vital standards 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.

Standard

1. GENERAL

This standard applies to all information security risk assessments that are conducted for SO information resources during the annual risk assessment process.

The intended audience includes *all SO personnel involved in performing, approving, or making risk management decisions* related to information security risk assessments.

2. STANDARDS

2.1 After completion of the annual risk assessment process (see Regulation 29.01.03), all assessment reports will be reviewed by SO ISO (i.e., the “primary review”). Based on the primary review, some assessments will be selected for additional review (i.e., a “secondary review”). The selection of assessments for secondary review and the order of these reviews will be predicated on areas of inherent risk (e.g., confidential information, mission critical systems, and/or problematic conditions) or at the direction of the Texas A&M University System Chief Information Officer (or designee).

2.2 The specific process followed for each review will be designed with effectiveness and efficiency as primary goals. 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 and/or mission critical data) of the information resources.

2.3 The review process shall include where appropriate: notification, information gathering, analysis, and reporting.

3. GUIDELINES

Detailed guidelines can be found at the DIR Risk Management website.

Related Statutes, Policies, or Requirements

Regulation 29.01.03

Contact Office

Contact the Texas A&M University System Chief Information Officer for standards interpretation or clarification

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer