29.01.99.K1.230 Risk Management of Information Resources Procedure

Effective: April 1st, 2004
Revised: April 25th, 2013
Revised: March 28th, 2019
Next Scheduled Review: March 2024

Introduction

A key component of an information security program is the recognition and management of potential security risks associated with the information resources at Texas A&M University-Kingsville (TAMUK).

Purpose

The purpose of this procedure is to outline the program phases which include risk analysis, risk assessment, and risk management required to fulfill this component.

Audience

This procedure applies to all individuals who use TAMUK Information Resources.

Risk Management of Information Resources Procedure

1. Inventory of Information Resources
   a. In the context of the risk management cycle, the primary objective of the inventory is to simply identify the information resource systems, their levels of criticality to University operations, and the individual who maintains ultimate responsibility for each system.
   b. iTech will maintain the list of information resources to be included in either the one-year or two-year risk management cycles. The inventory will depict a specific risk rating (High, Medium, Low) associated with each system. The risk rating will be based on definitions contained within the Texas Administrative Code §202 (TAC 202).

    c. In addition to the risk rating, the inventory should include at least the system name, its owner and custodian. More detailed and/or technical information will be collected during the analysis phase of the risk management cycle.

2. Risk Analysis
    a. The objective of the risk analysis phase of the risk management cycle is to identify the potential vulnerabilities or risks associated with the information resource, and then determine the potential likelihood and resultant impact of a security incident occurring due to the risk. This information will feed into the risk assessment phase.
    b. With the assistance of the system custodians, owners or their designated representatives will complete a standard questionnaire conforming to the requirements of TAC 202. The completed questionnaire will be submitted to the ISO, who may elect to expand the scope of the analysis based upon review of the questionnaire.
3. Risk Assessment
    a. The objective of the risk assessment phase is to assess potential options for reducing or mitigating vulnerabilities identified during the risk analysis.
    b. The system owner should be assisted by the custodian or other resources as appropriate to assess preferred solutions and associated cost and effort. In those instances where multiple risks have been identified for a single information resource, the security team will prioritize the execution of the solutions.
    c. At this point in the risk management cycle, the depicted costs and effort for risk reduction may be high-level estimates sufficient to assist in the prioritization process.
    d. The results of each information resource's risk assessment will be submitted to the ISO for eventual inclusion in the University's risk management plan.
4. Risk Management
   The objective of the risk management phase is to determine the actions necessary to most effectively reduce the threat of identified risks to individual information resources as well as the University in general.
5. The ISO is responsible for the following:
    a. Compile the risk assessments submitted by for each information resource owner. The assessments should be analyzed for common risks among multiple systems that may be reduced by shared solutions. These shared solutions should be incorporated in a risk management plan.
    b. Maintain a list of actions or projects identified during the risk assessment, and will track the progress of each.

This information should be consolidated and documented in a risk management plan to be submitted to the University president or his or her designated representative(s) annually. This plan must be formally approved by the president or representative (TAC 202.72).

Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution

References

1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
3. Computer Security Act of 1987
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
6. Foreign Corrupt Practices Act of 1977
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404