Travis County Technology & Security Policies

Risk Assessment Policy

Policy #: TC-ITS-217 **Approved By**: Paul Hopingardner, County Executive, Technology & Operations
Version #: 1.2 **Effective Date**: November 7, 2019

Accountability & Responsibility

This policy is governed by the Accountability and Responsibility policy found here.

Purpose

This Risk Assessment Policy empowers Travis County to perform periodic information security risk assessments (RAs) to determine areas of vulnerability and to initiate appropriate remediation. The identification of vulnerabilities and threats to Travis County information resources and identifying the likelihood and impact of successful attempts to compromise information resources, is critical to Agency function. Information Security will assess risk to the Agency based on National Institute of Standards and Technology (NIST) standards and controls.

Scope

Information Security Risk Assessments (RAs) may be conducted within Travis County or any outside entity that has signed a Third-Party Agreement with Travis County. RAs can be conducted on any Travis County information resource, to include applications, servers, and networks, and any process or procedure by which these systems are administered and maintained. Risk Assessments are ongoing processes that are dependent on the involvement of data owners and data custodians to be successful.

Policy

The execution, development, and implementation of the risk assessment process is the joint responsibility of Information Security and the department responsible for the system and data being assessed. Risk assessments can be the result of a need to update current vulnerabilities or assess future vulnerabilities. These vulnerabilities can be from systems, data, or persons.

The Risk Assessment Policy is in place to accomplish a universal understanding of the scope of a risk assessment and frequency.

The Risk Assessment Policy defines periodic assessments of the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of Agency information and information resources.

Risk Treatment

Risk Treatment refers to the range of choices available to management in handling a given risk.

Risk Treatment strategies include the following:

1. Risk acceptance involves assuming the potential loss associated with a given risk and making plans to cover any financial consequence of such losses. This can also include the inherent risk to the business.
2. Risk avoidance is a strategy utilized when a given risk poses a particularly serious threat that cannot be effectively reduced, and the conduct or service giving rise to the risk may perhaps be avoided.
3. Risk reduction or minimization involves various loss control strategies aimed at limiting the potential consequences or frequency of a given risk without totally accepting or avoiding the risk. Strategies may include staff education, policy and procedure revision, and other interventions aimed at controlling adverse occurrences without eliminating risk activities.
4. Risk Mitigation is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold.

Risk Assessment Methodology

The Risk Assessment will cover three phases:

1. Review of the IT Assessment;
2. Completion of the Risk Assessment; and
3. Review of the content provided from the Risk Assessment and follow up with the business unit to ensure mutual understanding of the current risk level and inherent impact, which will be classified as High, Moderate, or Low.

Employees are expected to cooperate fully with any RA being conducted on any information resource for which they are responsible. Employees are further expected to cooperate with Information Security (IS) in the development of system classifications and system definitions since any process without a control is an environment where risk may arise.

The Risk Assessment Methodology will utilize the RIIOT method: Review, Interview, Inspect, Observe, and Test.

Step 1: (Review) Based on the defined frequency for that resource, review all information resources based on their schedule for review.

Step 2: (Interview) Have each business unit complete their respective IT Assessment based on their criteria (data classification, dependencies, current climate, or as needed).

Step 3: (Inspect) Map the Information Resource to the Information Security protection

Step 4: (Observe/Test) Information Security will either observe end users interacting with their information resources or, in some cases, select a statistical sampling of responders to verify accuracy of reports. Information Security will confirm responses with data owners to ensure that the report is representative of actual user interaction.

Risk Assessment Frequency

Travis County will review systems and applications prior to a new implementation, prior to a significant change, and regularly based on current risks and priorities, not to exceed two years, to determine any changes in the acceptable levels of risk for information resources.

System Security Plans

Information Security should be addressed throughout the data's lifecycle. IS will work with Travis County's Project Management Office (PMO) to build security processes that are layered on top of the project management methodology.

- New Project: PMO will engage with IS during the Initiation Phase to ensure security safeguards and best practices are included.
  Input: Project Charter/Business Case, Functional Business Requirements
  Output: Defense against low to moderate security exploits
- Existing product or resource: PMO will engage with IS during the Initiation Phase to ensure security safeguards and best practices are included.
  Input: Project Charter/Business Case, Functional Business Requirements, Lessons Learned documentation
  Output: Defense against low to moderate security exploits

Exceptions

Within Travis County, any exception to the established Risk Assessment Policy must be documented and approved by the appropriate risk authority and tracked in the Risk Register.

Policy Revision

Version	Purpose/Changes	Editor	Date
1.0	Policy Creation	Larissa Derrick	07/02/2019

1.1	Approver title update and signed by PH	Brandon Rogers	11/07/2019
1.2	Added policy number.	Joyce Miller	11/20/2019