**Risk Management** **IT/PPS No. 04.15**

**Issue No. 5**

**Effective Date: 03/02/2023
Next Review Date: 03/01/2024 (EY)**

**Sr. Reviewer: Vice President for Information Technology**

**POLICY STATEMENT**

Texas State University is committed to the management of security risks posed to information resources.

1. **SCOPE**
	1. This policy establishes the Division of Information Technology (IT) risk assessment methodology to be applied to information security issues, identified infrastructure deficiencies, audit findings, observations, and recommendations impacting Texas State University information resources.
2. **RELATED DOCUMENTS**
	1. [UPPS No. 04.01.01](https://policies.txstate.edu/university-policies/04-01-01.html), Security of Texas State Information Resources
	2. [UPPS No. 04.01.11](https://policies.txstate.edu/university-policies/04-01-11.html), Risk Management of Information Resources
3. **DEFINITIONS**

03.01 Impact – the effect a single occurrence of a risk will have upon the achievement of the institution’s goals and initiatives.

03.02 Information Resources Manager (IRM) – the vice president for IT.

03.03 ISO – Information Security Office.

03.04 Probability – the likelihood that a risk will become reality.

03.05 Risk Assessment Methodology – a systematic process for describing and quantifying the risks associated with hazardous substances, processes, actions, or events.

03.06 Risk Register – a repository for all risks identified, including information about each risk (e.g., nature of the risk, reference and owner, and mitigation measures).

03.07 Risk Score – the impact and probability ratings used to create a final risk tally.

**04. GUIDELINES AND PROCEDURES**

04.01 As issues in an area arise (e.g., new audit report, new information security risk assessment, or other process or evaluation that surfaces a potential risk), these items should be categorized by their risk score, which is based upon a combination of probability and impact.

04.02 Issues will be documented, maintained, and managed by each associate vice president, or equivalent. If the issue is determined to be an information security incident or event, management of the incident will be handled by the ISO or, if classified by the ISO as high risk, the IRM.

04.03 The impact shall be classified by one of five values:

|  |  |
| --- | --- |
| Impact Value | Impact Description |
| Severe | The effect will cause the university to not achieve its goals and initiatives; it is an institutional showstopper. |
| Major | The effect will cause the component not to achieve its goals and initiatives; it is a showstopper. |
| Moderate | The effect will cause the university or component to operate inefficiently or expend unplanned resources to meet goals and initiatives. |
| Minor | The effects should be monitored to determine if action is required. |
| Insignificant | The measurable effect upon the achievement of university’s goals and initiatives would be immaterial or insignificant. |

04.04 The following factors, if pertinent to the risk, may be considered during the assessment of impact: human health and safety, societal or environmental, monetary, business or operations, information technology, information security, public relations, reporting and disclosure, strategic, compliance, and fraud.

04.05 The matrix shall classify the probability with one of five values:

|  |  |
| --- | --- |
| Probability Value | Probability Description |
| Almost Certain | An event is inevitable, or there is a great likelihood that an event will occur. |
| Likely | An event will probably occur. |
| Possible | The risk is neither extremely likely nor highly unlikely. The probability of an event is similar to occurrences within the normal course of operations. |
| Unlikely | The risk of an event is not anticipated. |
| Rare | The risk of an event is extremely unlikely or would require a combination of multiple failures. |

04.06 The following factors, if pertinent to the risk, may be considered during the assessment of probability:

1. history;
2. conflicts of interest;
3. susceptibility to fraud or theft;
4. key changes (including leadership, key personnel, regulations, policies, operating processes, computer systems, software applications);
5. control activities need improvement;
6. policies and procedures require updates;
7. training; and
8. complexity of unit or process.

**05. PROCEDURES FOR CALCULATING RISK SCORE**

05.01 The impact and probability ratings are used to create a quantitative calculated risk score encompassing a range from 1 to 25 (R = P x I). Higher scores indicate increased risk.

05.02 Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Probability | Almost Certain | 5 | 10 | 15 | 20 | 25 |
| Likely | 4 | 8 | 12 | 16 | 20 |
| Possible | 3 | 6 | 9 | 12 | 15 |
| Unlikely | 2 | 4 | 6 | 8 | 10 |
| Rare | 1 | 2 | 3 | 4 | 5 |
|   | Insignificant | Minor | Moderate | Major | Severe |
|   |   | Impact |

05.03 Risk scores are classified into five categories to assist in determining the need for, or immediacy of, response or action.

|  |  |  |
| --- | --- | --- |
| Risk Classification | Action Required | Calculated Risk Score |
| Catastrophic | Immediate Action | 16 - 25 |
| Critical | Urgent Action | 10 - 15 |
| Moderate | Action Needed | 5 - 9 |
| Low | Monitor | 3 - 4 |
| Insignificant | No Action | 1 -2 |

**06. PROCEDURES FOR APPLYING RISK SCORES TO AUDITS AND DEPARTMENTAL RISK ASSESSMENTS**

**06.01 Calculated risk scores should be included, where appropriate, in any risk assessment performed by departments of the Division of IT.**

**06.02 Calculated risk scores should be included in response to any audit finding, recommendation, observation, or area of improvement. When appropriate, this risk score will guide the management response.**

**06.03 Calculated risk scores should be maintained in each IT department’s risk register, which should be updated regularly.**

**07. REVIEWERS OF THIS PPS**

**07.01 Reviewers of this PPS include the following:**

**Position Date**

Special Assistant to the March 1 EY

Vice President for Information

Technology

Associate Vice President, March 1 EY
Information Technology Assistance

Center

Director, March 1 EY
Information Technology Business

Operations/Services

Director, March 1 EY

Information Technology Business

Operations/Finance

Associate Vice President, March 1 EY

Technology Innovation Office

Associate Vice President, March 1 EY
Technology Resources

Chief Information Security Officer March 1 EY

Executive Assistant, Information March 1 EY

Technology

Vice President for Information March 1 EY

Technology

**08. CERTIFICATION STATEMENT**

This PPS has been reviewed by the following individual in their official capacity and represents Texas State Information Technology policy and procedure from the date of this document until superseded.

Vice President for Information Technology; senior reviewer of this PPS