ISAAC
Non-Confidential Assessment
• ISAAC Assessment is available at:  
  https://isaacs.tamu.edu/

• ISAAC is licensed from Texas A&M (TAMU), therefore you will see references to TAMU throughout the assessment sections. These references are hard coded, but logically you can substitute Texas State University wherever you see TAMU.

• Please refer to the ISAAC Glossary provided to look up terms used in this assessment tool
New Users: Create User ID and Password

Registered Users: Login
(Contact IT Security if you do not remember your UserID or Password)
• Complete this form to create your User ID. All fields are required
• Select Texas State under TAMU Component *(this is a critical step, if you select another TAMU component your assessment cannot be verified)*
• Select both check boxes for Systems Security and Systems Administrator
Choose Confidentiality Option (see ISSAC Glossary for definitions)

Classification of Departmental Information abc systems.

Please read the following description, and answer the following question carefully.

The Texas Department of Information Resources defines CONFIDENTIAL data as:
"Information that is excepted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal law."

Some examples of Confidential data are provided below:

- Information contained in education records of an educational agency or institution, except in conformity with the Family Educational Rights and Privacy Act of 1974.
- Information in a personnel file, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.
- Test items developed by an educational institution.

See 552.022, Categories of Public Information: Examples or the Privacy Statutes Chart for a more detailed list of confidential data examples.

**QUESTION SCENARIO 1:** If the only confidential data a department accesses is a centralized payroll or student information system, etc. (and no data is downloaded or extracted to a local database or spreadsheet), then the department does not "own and maintain" the confidential data.

**QUESTION SCENARIO 2:** If a department maintains data which includes student grades in a local database [such as MS Access or Oracle], then the department does "own and maintain" confidential data.

**Does VPIT own and maintain CONFIDENTIAL data?**

- Yes
- No

Select Option and Click ‘Next’
Select Mission Critical Option (see ISSAC Glossary for definitions)

Classification of Departmental Information abc systems.

Please read the following description, and answer the following question carefully.

Based on the Texas A&M Security Standards definition, MISSION CRITICAL data is defined as:
"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."

Some examples of Mission Critical data are provided below:

- If data loss impacts the department’s ability to teach, perform research, or provide essential services.
- If data loss causes harm to the life, safety, or financial well being of faculty, staff, students or the community.
- NOT mission critical if data loss only incurs an inconvenience to the department.

QUESTION SCENARIO 1: If a department’s loss of data could cause an impact on the department’s ability to teach, perform research, or provide essential services, then the department does “own and maintain” mission critical data.

QUESTION SCENARIO 2: If a department’s loss of data could be circumvented by manual means (e.g. paper and phone), then the department probably does not “own and maintain” mission critical data.

Does VPIT own and maintain MISSION CRITICAL data?

[Yes] [No]

Select Option and Click ‘Next’
• Click on View & Create Assessments

(Note: Do not use any other section)
• If you completed a 2010 Risk Assessment, then a 2011 Assessment has already been started for you using the responses supplied the previous year
• The new assessment will be transferred to your account and you can find it under ‘Created Assessments’
• If you have not previously assessed your servers you must create a new Risk Assessment
• Naming Convention: Year Department Function
  Example: 2011ITSecurityWebServer
• Select Desktops or Server/Clients and click ‘Create’
• If creating a new assessment, you must answer the Confidential and Mission Critical questions at the beginning

• If a 2011 assessment has already been created for you, please verify each response is still applicable and correct before continuing

• After completing each page, click on the button at the bottom of the page marked with the next section
• Complete Sections A, B, and C
  – *Section D and D2 are optional*

• All Narrative and Comment sections are optional

• **The following screen shots include some pre-determined answers identified by IT Security. Please select the response as it is described.**
Section A: Questions A5 and A6

Include **ALL** users in your Department for the “Users Supported” and “Security Awareness Training” questions (A5 and A6)
Section B: Questions B1-A, B1-D, and B1-E

B1- A) Select ‘**Yes**’ if the standard workstation image is used

B1- D) Select ‘**Yes**’ – Vulnerability scanning is performed by IT Security

B1- E) Vulnerability Scan Frequency: Select ‘**Bi-annually**’

---

**Acquisition, Development and Testing of Information Systems**

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are new systems secured* before connecting them to the TAMUS network?</td>
<td>Yes or No</td>
</tr>
<tr>
<td>(* i.e., remove unnecessary services, restrict access, apply updates, patches, etc.)</td>
<td></td>
</tr>
<tr>
<td>Are security logs and audit controls included in the configuration of new information systems?</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Do you implement security patches and fixes as soon as they are announced?</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Do you periodically scan for vulnerabilities on your information systems (using your own vulnerability scanning software or by requesting the service from a third party)?</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Please indicate the frequency in which you conduct (or request a third party for) vulnerability scans.</td>
<td>Annually, Bi-annually, Monthly, Weekly, Random (event driven), Never</td>
</tr>
</tbody>
</table>
Select ‘Yes’ – IT Security investigates all suspected security incidents and documents according to DIR requirements.
• On the Assessment Results page, be sure to click the “Report Results” button

This is a critical step: if you do not generate the report, your updated assessment will not be submitted
• Use the **Navigation Menu** to go back to the **Main screen** once you have completed the assessment

• Click on ‘View & Create Assessments’

• Scroll down to ‘Created Assessments’

• Check the box and **click Status Update**

• Notice that the **Current Status** will display the current date
Contacts

• Contact IT Security if you have any questions completing your assessment

• Contact IT Security if you forget your User ID or password

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lori McElroy</td>
<td>Rick Myers</td>
<td>Kyle Colson</td>
<td>IT Security</td>
</tr>
<tr>
<td><a href="mailto:lori.mcelroy@txstate.edu">lori.mcelroy@txstate.edu</a></td>
<td><a href="mailto:rm73@txstate.edu">rm73@txstate.edu</a></td>
<td><a href="mailto:kc1417@txstate.edu">kc1417@txstate.edu</a></td>
<td><a href="mailto:itsecurity@txstate.edu">itsecurity@txstate.edu</a></td>
</tr>
<tr>
<td>X5-7885</td>
<td>X5-4736</td>
<td>X5-4225</td>
<td>X5-4225</td>
</tr>
</tbody>
</table>