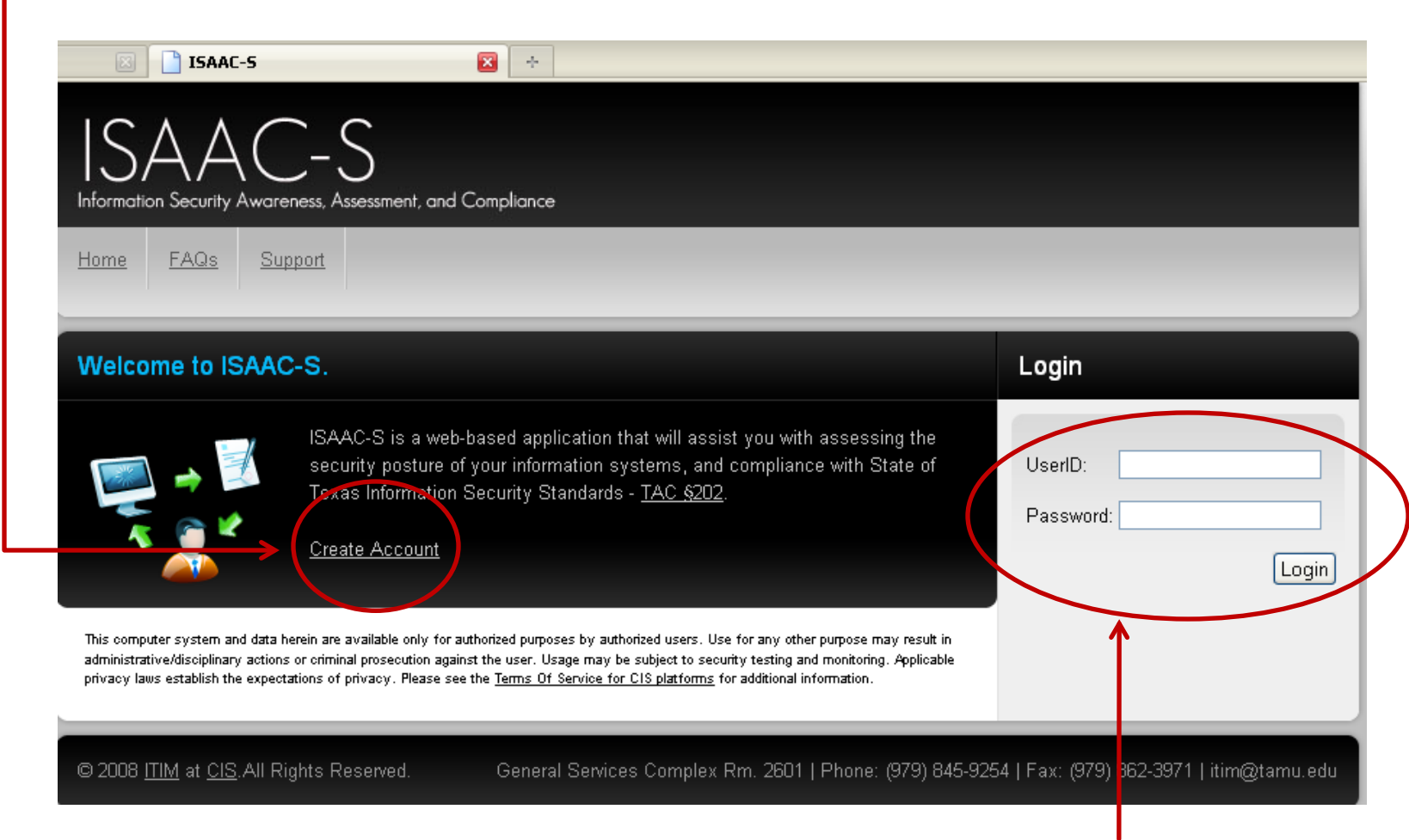


ISAAC Assessment

- ISAAC Assessment is available at:
<https://isaacs.tamu.edu/TAC/index.cfm>
- ISAAC is licensed from Texas A&M (TAMU), therefore you will see references to TAMU throughout the assessment sections. You can substitute Texas State University wherever TAMU is referenced.
- Please refer to the ISAAC Glossary provided to look up terms used in this assessment tool
- First time users: Will need to register to access the assessment tool (see following slides)

New Users - Create User ID and Password



Login, if you are a Registered user

1. Complete this form to create your User ID. All fields are required
2. Select Texas State under TAMU Component
3. Select both check boxes for Systems Security and Systems Administrator

New Account Creation

TAMUS Component: TAMU Commerce ▼

First Name
Add your first name

Last Name
Add your last name

Title
Add your title

Departments
Add your department's name

Postal Address
Add a valid address

Mail Stop
Add a valid mail stop

Email Address
Add a valid email address

Phone
Add a phone number

Role Verification. I am the Information Systems Security Administrator.
Check role(s)

I am the Information Systems Administrator.

UserID:
Create your UserID.

Password
8 characters max,
special characters will be
removed

Password Verification
Retype the password.

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 abc own and maintain CONFIDENTIAL data?

Yes No

Next →

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 abc own and maintain MISSION CRITICAL data?

Yes No

Next →

Select Option and Click 'Next'

Login with your new UserID and Password

Click on View & Create Assessments

ISAAC-S Dashboard.

Account Management



Update contact and department information regularly. Click here to check.

MORE

Register Resources



It is important to keep a listing of your resources. Make sure you list is current.

MORE

View & Create Assessments



Ready to assess resources? View and create assessments here.

MORE

User Resources

[Security Training](#)

Increase knowledge. ▶ View links to IT security training sites.

[Business Continuity Planning](#)

Be prepared. ▶ Create a BCP and/or DRP with this guide from Texas DIR.

[Physical Security Safeguards](#)

Secure your resources. ▶ Ensure the physical security to IT equipment.

[Templates & Guides](#)

Forms & Guides. ▶ Common IT forms and documents.

[Activity Summary](#)

Registered Resources

No Resources Registered.

Type a name for your assessment

Select Desktops or Server/Clients and click Create

Create a New Risk Assessment.

In order to create a new Risk Assessment, you must first determine if your departmental systems store, transmit, or maintain mission critical and/or confidential information. Additionally, you will need to determine if you are assessing risk for a server and all clients or for a collection of desktop systems that are connected to the network individually (or in a peer-to-peer fashion) with no dedicated server. You may create as many assessments (and types of assessments) as necessary to include ALL of your information systems.

For an overview of the risk assessment module, please see the [Purpose](#) section below.

Assessment Name:

**special characters will be removed

Risk Assessment Focus:

Desktops

Server/Clients

Create

- Answer Confidential and Mission Critical questions at beginning of each assessment
- After completing each page, click on the button at the bottom of the page marked with the next section
 - Example: At the end of Section A, click on the button ‘Section B’
- Non-Confidential Assessments:
 - Complete Section A, B, and C. Section D and D2 are optional.
- Confidential Assessments:
 - Complete Section A, B, C and D. Section D2 is 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 (disregard the actual numbers).

Section A:

A3. Please provide the common name(s) used to reference the Information Systems (similarly configured) for this assessment.

A4. Data Classification Types:

Mission Critical Confidential

A5. What Building(s) house the Information Systems?

A6. How many servers are included in this assessment?

A7. How many users do the Information Systems support (including administrators)?

A8. How many users have received computer security awareness training (including administrators)?

(Introductory) (In-depth)

A9. Check the boxes that reflect the types of data maintained on the Information Systems:

Include all users in your Department for the “Users Supported” and “Security Awareness Training” questions (these questions are numbered differently, depending on whether you are completing a Confidential or Non-Confidential assessment)

Section B:

Acquisition, Development and Testing of Information Systems

Attributes

A) Are test functions kept either physically or logically separate from production functions?	<input type="radio"/> Yes <input checked="" type="radio"/> No
B) Are copies of production data used for testing only if the data owner has agreed, or all departmental and contractor employees involved in testing are authorized to access the data?	<input type="radio"/> Yes <input checked="" type="radio"/> No
C) Are information security and audit controls included in all phases of the information systems development lifecycle or acquisition process?	<input type="radio"/> Yes <input checked="" type="radio"/> No
D) Are all security-related information resource changes approved by the data owner through a quality assurance process before implementation? (must be approved by owner prior to implementation)	<input type="radio"/> Yes <input checked="" type="radio"/> No
E) Do you implement patches and fixes discovered as a result of periodic, vulnerability scanning of your systems?	<input type="radio"/> Yes <input checked="" type="radio"/> No
F) Please indicate the frequency in which you conduct vulnerability scans.	<input type="radio"/> Annually <input checked="" type="radio"/> Bi-annually <input type="radio"/> Monthly <input type="radio"/> Weekly <input type="radio"/> Random (event driven) <input type="radio"/> Never
G) Please indicate the typical amount of time between vendor announcement and/or discovery of a vulnerability and implementation of a patch, fix, or other remedial action.	<input type="radio"/> Same Day <input type="radio"/> Within 2 Days <input type="radio"/> 1 Week <input type="radio"/>

Vulnerability Scan Frequency: Select 'Bi-annually'

Section E for Confidential Assessments – Complete all Corrective Action sections including Target date and Responsible Party:

Section E: Documentation of corrective actions and risk management decisions.

— Navigation Menu —

A corrective action plan (with target completion dates and cost estimates) is required to address deficiencies noted during this risk assessment. This automated risk assessment will outline what corrective action plans are required for meeting TAC 202 compliance below.

Some EXAMPLE deficiency areas that are KEY include:

1. Software and/or data backups are not maintained (a response of "None" in Item B1);
2. The effectiveness afforded the information systems does not result in a "Moderate" or higher rating (Item B3),
3. Any required countermeasure is not implemented (a response of "No" in Section C at or below security level designated)
4. There is no Business Continuity / Disaster Recovery Plan (Item D2) or there is a Plan, but it does not include the required items listed in Item D3.

You have 38 Corrective Action items.

Item B1a. Backup Frequency of Software (non-commercial applications):

Corrective Action:

Risk Management Decision:

Estimated Cost:

Target Completion Date:

Responsible Party:

Item B1b. Backup Frequency of Data:

- 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

Your previously created risk assessment, are shown below for you to edit. Just click on the name of the assessment that you want to edit.

You may mark only one assessment at a time as completed.

NOTE: For each Risk Assessment, "Completed" indicates that the Department Head has read the risk assessment report and has accepted and certified the results by signing the report.

Created Assessments

Departmental Risk Assessment	Completion Status
Newtest2009	Current Status: Not Completed
Rename	Completed? <input type="checkbox"/> Status Update
	<input type="checkbox"/> Check here to mark assessment for deletion then click on the "Status Update" button above.

- 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

Lori McElroy

lori.mcelroy@txstate.edu

X5-7885

Corbett Consolvo

cc72@txstate.edu

X5-2701

IT Security

itsecurity@txstate.edu

X5-4225