

ISAAC-S

1. Does (Organization) own and maintain CONFIDENTIAL data?
(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.)
2. Does (Organization) own and maintain MISSION CRITICAL data?
(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.)

Section A - Administrative Information for Information Systems

All fields are required in Section A.

A1. Information Systems Security Administrator (ISSA):

First Name: Joe

Last Name: Green

E-mail Address: joe.green@ttuhsc.edu

Postal Address: 3601 4th Street, Lubbock, TX 79430

Phone Number (office): 806-743-1500

Joe Green's information is entered here

A2. Information Systems Administrator (ISA):

First Name: _____

Last Name: _____

E-mail Address: _____

Postal Address: _____

Phone Number (office): _____

Your information is entered here

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:
- Administrative - General correspondence and information (e.g., property records and H.R or personnel information generally available to public).
 - Financial - Budget and expenditure information relating to departmental operations.
 - Grant/Contract - Information relating to departmental grants and contracts.
 - Research - Information resulting from or used to support departmental research activity.
 - Private or Confidential - Information (not generally available to the public) required to be protected, such as student records under the Family Educational Rights & Privacy Act (FERPA) and staff and faculty records under the Privacy Act of 1974, Public Law 93-579, 5 U.S.C. 552a (1974).

HIPAA Covered Entities - Only check the HIPAA EPHI option below if you are considered a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA). You will be required to complete an additional HIPAA Security Rule compliance module by checking this option.

HIPAA EPHI - HIPAA Electronic Protected Health Information (EPHI) is individually identifiable health information that is transmitted or maintained by electronic media (excluding education records covered by the Family Educational Rights & Privacy Act (FERPA) and employment records). See formal definition in the Glossary.

PCI Covered Entities - Only check the PCI option below if you process credit card transactions are subject to the Payment Card Industry (PCI) Data Security Standard (DSS). You will be required to complete an additional PCI Security Rule compliance module by checking this option. NOTE: If you check the PCI option below, the data on the information systems will be considered both Mission Critical and Confidential.

PCI DSS The Payment Card Industry (PCI) Data Security Standard (DSS) is a broad-based security standard which describes a range of cross-business security functions and procedures which are required to ensure the security of payment cardholder data. See formal definition in the Glossary.

Other (please specify - 250 char. max)

A10. Information Systems Asset Valuation - "The expense of security safeguards must be commensurate with the value of the assets being protected" (from Texas State Information Security Standards)

NOTE: For this analysis, please enter either the "total cost range" -OR- the unit replacement cost. Also, the item descriptions below are only suggestions and can be modified to suit your environment.

Please enter decimal values only (e.g., no \$ signs or commas) for the "Quantity" and "Replacement Cost" categories.

Quantity	Item Description	Replacement Cost (per unit)	OR	Total Cost Range
0	Windows based Server		OR	Not Selected Very Low < \$25000 Low \$25001-\$50000 Moderate \$50001-\$250,000 High \$250,001-\$500,000 Very High
0	Unix based Server		OR	- Same as above -
0	Other Server Type		OR	- Same as above -
0	Windows based Workstations		OR	- Same as above -
0	Unix based Workstations		OR	- Same as above -
0	Mac based Workstations		OR	- Same as above -
0	Other Workstation Types		OR	- Same as above -
0	Uninterruptible Power Supply		OR	- Same as above -
0	Printers		OR	- Same as above -
0	Wireless Access Point		OR	- Same as above -
0	Portable Devices		OR	- Same as above -
0	Other Equipment		OR	- Same as above -

A11. Indicate the date of the last risk assessment

Month ___ Year ___ OR Check here if this is an initial risk assessment

Section B – Departmental Information Systems Characterization

All fields are required in Section B.

B1. Frequency of backup for data and software (non-commercial applications) on the server.

	Daily	Weekly	Monthly	On install or modify	None
Software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remember to unselect "None" if selecting other options

* If "None" is checked (or all are left unchecked), you will have to create a Corrective Action plan in Section E.

B2. Now, consider the sensitivity and processing criticality of your data in rating the need for protection in the following three categories: confidentiality; integrity; and availability. You may click on each category below for a more detailed explanation.

	Confidentiality	Integrity	Availability
Low			
Moderate			
High			

B3. Using the scale and criteria below, check the rating which best reflects the effectiveness of the Information Resources safeguards.

Effectiveness of Information Systems Protection

RATING	CRITERIA
Very Low	Daily problems with Information Systems availability are encountered and/or very little, if any, assurance of maintaining data integrity and/or data confidentiality.
Low	Problems with Information Systems availability are not uncommon and/or limited assurance of maintaining data integrity and/or confidentiality.
Moderate*	Information Systems normally available to support operations and data integrity and/or confidentiality are well protected.
High	Information Systems rarely unavailable and data integrity and confidentiality are well protected.
Very High	Information Systems availability and data integrity and confidentiality are assured.

*** If not at least "Moderate", the Information Systems are considered to be inadequately protected.**

B4. Please answer the following questions related to information systems development and testing.

Acquisition, Development and Testing of Information Systems

A) Are test environments kept either physically or logically separate from production environments?	Yes No
B) Are copies of production data used for testing only if the data has been authorized for public release or all custodians involved in testing are otherwise authorized to access to the data?	Yes No
C) Are information security, security testing and audit controls included in all phases of the information system development lifecycle or acquisition process?	Yes No
D) Are all security-related information resource changes approved by the data owner through a change control process before implementation by the institution of higher education or independent contractors?	Yes No
E) Do you implement patches and fixes discovered as a result of periodic, vulnerability scanning of your systems?	Yes No
F) Please indicate the frequency in which you conduct vulnerability scans.	Annually Bi-annually Monthly Weekly Random (event driven) 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.	Same Day Within 2 Days 1 Week 2 Weeks 1 Month Never
H) Are devices designed for public access (e.g., kiosk systems or computer labs that do not require authentication) configured to enforce security policies and procedures without the requirement for formal acknowledgement? (NOTE: Only choose "N/A" [not applicable] if you do not have ANY publicly accessible systems.) (NOTE: Only choose "N/A" (not applicable) if your department does not have ANY publicly accessible systems)	Yes No N/A

I) With regard to the disposal or transfer of data processing equipment and storage devices, if it is POSSIBLE that the storage device contains confidential information, restricted personal information, mission critical information, intellectual property or licensed software, is the storage device either (A) removed and destroyed or (B) sanitized via methods compliant with the DIR guidelines for the sale or transfer of computers and software? (http://www.dir.state.tx.us/pubs/saleortransfer/saleortransfer.htm)	Yes No <div style="border: 1px solid red; padding: 5px; color: red; text-align: center;">For more info see OP 63.10</div>
J) Is the destruction of electronic state records in accordance with 441.185, Government Code, and, if the record retention period has not expired, are copies of the data retained for the required retention period?	Yes No
K) Are records kept documenting the removal of data, including the date, description of the item(s) and serial number(s), inventory number(s), the process and sanitization tools used or the method of destruction, and the name and address of the organization to which the equipment was transferred?	Yes No
L) Are new systems secured (e.g., unnecessary services removed, access restricted, default passwords changed, patched, etc.) before connecting them to the institution's network?	Yes No
M) Are security requirements identified, documented and addressed in all phases of development or acquisition of information resources?	Yes No

B5. Please answer the following questions related to the responsibilities of the information system(s) owner.

Responsibilities of the Information System(s) Owner

Owner Responsibilities (or Designee)

A) Does the information resource(s) owner or designated representative(s) approve access and formally assign custody of the information resources asset?	Yes No
B) Has the information resource(s) owner or designated representative(s) determined the information resources asset's value?	Yes No
C) Does the information resource(s) owner or designated representative(s) specify data control requirements and convey them to users and custodians?	Yes No
D) Does the information resource(s) owner or designated representative(s) specify appropriate controls, based on a risk assessment, to protect the information resources from unauthorized modification, deletion, or disclosure, including those information resources and services outsourced by the institution of higher education?	Yes No

E) Does the information resource(s) owner or designated representative(s) confirm that controls are in place to ensure the confidentiality, integrity and availability of data and other information resources?	Yes No
F) Does the information resource(s) owner or designated representative(s) assign custody of the information resources assets and provide appropriate authority to implement security controls and procedures?	Yes No
G) Does the information resource(s) owner or designated representative(s) review access lists based on documented security risk management decisions?	Yes No

H) Does the information resource(s) owner or designated representative(s) approve, justify, document, and assume accountability for exceptions to security controls and coordinate such exceptions with the information security officer or other person(s) designated by the agency head?	Yes No
I) Has the information resource(s) owner classified business functional information (with the concurrence of the state agency head or designated representative)?	Yes No

B6. Please answer the following questions related to the responsibilities of the information system(s) custodian (typically the system administrator).

Responsibilities of the Information System(s) Custodian

Custodian Responsibilities

A) Does the information resource(s) custodian (including third party entities providing outsourced information resources services) implement the controls specified by the owner(s)?	Yes No
B) Does the information resource(s) custodian (including third party entities providing outsourced information resources services) provide physical, technical and procedural safeguards for the information resources?	Yes No
C) Does the information resource(s) custodian (including third party entities providing outsourced information resources services) assist the owner(s) in evaluating the cost-effectiveness of controls and monitoring?	Yes No
D) Does the information resource(s) custodian (including third party entities providing outsourced information resources services) implement monitoring techniques and procedures for detecting, reporting and investigating incidents?	Yes No

All fields are required in Section C.

Section C: Required Countermeasures

Note: Your required Security Level is HIGH (as determined by the highest rating checked in B2). Please answer "Yes" or "No" to ALL of the following required countermeasures below (Note: a "Yes" response to all countermeasures for HIGH and below are required in order to achieve full compliance with state security standards).

A Security Level color key is provided: Low Med. High

Countermeasures:	Yes No NA
C1. Do information systems contain authentication controls (i.e., UserID and Password) or other mechanisms to prevent unauthorized use?	Yes No
C2. Are appropriate audit trails maintained to provide accountability for all changes to automated security or access rules?	Yes No
C3. Do all information resources that process confidential information provide the means for auditing and establishing individual accountability for actions that can potentially cause access to, generation of, modification of, or effect the release of confidential information?	Yes No
C4. Are appropriate audit trails maintained to provide accountability for updates to mission critical information, hardware and software?	Yes No
C5. Are backups of mission critical data stored off-site in a secure, environmentally safe, locked facility that is accessible only to authorized state representatives?	Yes No
C6. For facilities in which information resources are housed, are environmental control procedures and equipment monitored by employees trained in both monitoring and emergency procedures?	Yes No
C7. Have written emergency procedures been developed, and are they updated and tested at least annually?	Yes No
C8a. Is all confidential information accessible only to authorized users and protected in its entirety?	Yes No
C8b. Are all information files or records containing any confidential information identified and documented (e.g., ISAAC Resource Registration module)?	Yes No
C9. For information resource systems that use passwords (e.g., operating systems, applications, etc.), are those passwords based on industry best practice and documented agency risk management decisions?	Yes No
C10. Is physical access to mission critical information resources facilities managed and documented to ensure the protection of information resources from unlawful or unauthorized access, use, modification or destruction, and reviewed at least annually as part of the risk assessment process?	Yes No
C11. If a user's employment or job responsibilities change, is that user's access authorization appropriately modified or removed?	Yes No

C12. Are security incidents (e.g., suspected intrusion, illegal activity, or unauthorized activity) promptly assessed, investigated, documented, and reported in accordance with TAC 202 security incident reporting requirements?	Yes No
C13. Do all system identification/logon banners have warning statements that include the following topics: unauthorized use is prohibited; usage may be subjected to security testing and monitoring; misuse is subject to criminal prosecution; and users have no expectation of privacy except as otherwise provided by applicable privacy laws?	Yes No
C14. Are users of the information resources assigned a unique identifier (i.e., User ID), except where risk analysis demonstrates no need for individual accountability of users, and authenticated prior to being granted access?	Yes No
C15. Does the agency provide an ongoing information security awareness education program for all users?	Yes No
C16. Are the information resources protected from environmental hazards (e.g., extreme temperatures, humidity, dust, static electricity, etc.)?	Yes No
C17. Do tasks that are susceptible for fraudulent or other unauthorized activity have adequate controls (i.e., procedures) and appropriate separation of duties?	Yes No
C18. Have all authorized users of the information resources formally acknowledged that they will comply with the security policies and procedures of the agency? Users include, but are not limited to, agency personnel, temporary employees, and employees of independent contractors.	Yes No
C19. Has the agency head or designated representative and the information security officer established a strategy for the use of written non-disclosure agreements to protect information from disclosure by employees and contractors prior to granting access?	Yes No
C20. Does new employee orientation introduce information security awareness and inform new employees of information security policies and procedures?	Yes No
C21. Based on risk assessment, is a sufficiently complete history of transactions maintained to permit an audit of the information resources by logging and tracing the activities of individuals through the system?	Yes No
C22. Are information resources assigned to another state agency, a contractor or another third party protected in accordance with the conditions imposed by the providing agency?	Yes No
C23. Is the use of encryption for transmission and storage of information based on documented agency risk management decisions?	Yes No
C24. Is all confidential information transmitted through a public network (e.g., the Internet) encrypted?	Yes No
C25. Are changes made to data only in an authorized manner, in order to ensure the integrity of the data, its source, its destination and processes applied to it?	Yes No

C26. Are inactive user accounts disabled after a specific period of time (e.g., 3 or 4 months)?	Yes No
C27. For virus susceptible platforms (e.g., Microsoft and Mac), is anti-virus software set to scan files automatically, and are virus signatures updated routinely? (NOTE: Only choose "N/A" [not applicable] if this assessment does not include ANY virus susceptible platforms.)	Yes No
C28. Is the building fire emergency preparedness plan available for review by the Information Systems Administrator?	Yes No
C29. Is anti-spyware software kept up to date and used to scan susceptible systems frequently?	Yes No
C30. Is an alternate source of power (e.g., emergency bus supplied by the building emergency generator and/or UPS) provided?	Yes No
C31a. Do mission critical and/or confidential software provide features to automatically lockout a workstation if inactive for more than a reasonable time?	Yes No
C31b. Do mission critical and/or confidential software provide features to automatically lockout a workstation if a password is not entered correctly after a specified number of attempts?	Yes No
C32. Are confidential data files encrypted on portable systems (e.g., laptops, PDAs, and tablet PCs)?	Yes No
C33. If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?	Yes No
C34. Are there procedures for ensuring that only authorized users pick up, receive, or deliver confidential input and output information and media?	Yes No
C35. Is the operating system configured to prevent circumvention of the security software and application controls?	Yes No
C36. Are procedures in place to determine compliance with password policies?	Yes No
C37. Are integrity verification mechanisms (e.g., data integrity assurance software, form field checking, or exception processing) used in order to discover evidence of and/or prevent data tampering, errors and omissions?	Yes No
C38. Are procedures in place to prohibit circumventing password entry with auto-logon, application remembering, embedded scripts or hard-coded passwords in client software for systems that process/store mission critical and/or confidential data?	Yes No
C39. Are passwords distributed securely and are users informed not to reveal their passwords to anyone (social engineering)?	Yes No
C40. If wireless access points are used, are adequate encryption (e.g., VPN or WEP/WPA) and authentication (e.g., RADIUS server) mechanisms in place to secure the wireless transmissions?	Yes No
C41. Are individuals who are authorized to bypass significant technical and operational controls evaluated prior to access and periodically thereafter?	Yes No
C42. Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., UDP, FTP, Telnet, mainframe supervisor calls)?	Yes No

Section D: Information Systems Environment and Procedures

D1. Facility environment and services available (check all appropriate blocks):

- Guards
- Receptionist
- Visitor escort
- Identification required
- Environmental Monitoring/Control > Last Tested: **Constantly monitored / calibrated annually**
- Emergency Generator Power -> Last Tested: **Tested Monthly**
- Uninterruptible Power Supply (UPS) -> Last Tested: **N/A**
- Fire Detection -> Last Tested: **Tested Annually**
- Fire Suppression **N/A**

Leave this section blank. Since we do not have specific date available, the field should be left blank.

Maintenance support for Information Systems:

- Hardware (to include spares) Software

D2. When was the Business Continuity Plan (including the Disaster Recovery Plan) last reviewed and/or updated? _____ No plan Available

D3. Is the BCP approved by the agency head or designated representative and has it been distributed to key personnel with a copy stored off-site? Yes/No

D4. Business Continuity / Disaster Recovery Plan

In determining your compliance with state information security standards for maintaining a Business Continuity / Disaster Recovery Plan, you need to consider if the IT resources are truly mission critical.

For example, consider the following:

1. Will the agency be able to continue to accomplish its mission without the IT resource?
2. Will the department be able to continue to accomplish its mission without the IT resource?

3. Will the department be able to continue to fulfill contract or grant related obligations in a timely manner without the IT resource?
4. Will the department be able to continue to conduct teaching and research activities without the IT resource?

If you answer "yes" to Question 1, then the IT resource is not mission critical to the agency.

If you answer "yes" to Questions 2, 3, or 4, then the IT resource may not be mission critical to your department.

If you answer "no" to any of the above questions, then you need to consider how long the IT resource can remain unavailable (waiting on recovery, restoration, etc.). Also, if you will be unable to restore IT services within the time frame that you determine, you will need to provide an alternate process or manual method(s) to continue critical business and services. Your recovery strategy for the IT services should be included in your department's Business Continuity Plan.

Typically, the IT team maps the recovery of the IT resources for business function recovery (sometimes at an alternate site). You may need to consult your Department Head on how they would like to incorporate the IT recovery strategy into the Departmental Business Continuity Plan. The size and complexity of the BCP will depend on the number of mission critical processes the department has, and should be based on risk management decision.

1.) Mission critical information resources?	Yes No
2.) Internal and external points of contact for personnel that provide or receive data or support interconnected systems?	Yes No
3.) Supporting infrastructure such as electric power, telecommunications connections, and environmental controls?	Yes No
4.) Disruption impacts and allowable outage times?	Yes No
5.) The effects of an outage over time to assess the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function?	Yes No
6.) The effects of an outage across related resources and dependent systems to assess cascading effects on associated systems or processes?	Yes No
7.) Recovery priorities that consider geographic areas, accessibility, security, environment, and cost and may include a combination of (1) preventive controls and processes such as backup power, excess capacity, environmental sensors and alarms and (2) recovery techniques and technologies such as backup methodologies, alternate sites, software and hardware equipment replacement, implementation roles and responsibilities?	Yes No
8.) Does the BCP include a risk assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action?	Yes No
9.) Does the BCP include an implementation, testing and maintenance	Yes No

management program that addresses the initial and ongoing testing and maintenance activities of the plan.	
10.) Does the DRP contain measures which address the impact and magnitude of loss or harm that will result from an interruption?	Yes No
11.) Does the DRP identify recovery resources and a source for each?	Yes No
12.) Does the DRP contain step-by-step instructions for implementing the plan?	Yes No
13.) Does the DRP include provisions for annual testing?	Yes No

Answer the following questions based on your current knowledge

D5. Provide a narrative of the controls used to ensure the integrity of the network access software and shared applications: _____

D6. Briefly describe the measures used to control access privileges for: reading, modifying and deleting files: _____

D7. Briefly describe the measures used to control access privileges for remote user access: _____

D8. Briefly describe the virus protection provided for the Information Systems (including frequency of updates): _____

D9. Describe the protection afforded the Information Systems closets and cabling _____

D10. Describe the smoke and fire detection/suppression system for the building(s) where the Information Systems are located: _____

D11. Describe any additional methods used to emphasize computer security awareness: _____

D12. Describe any additional safeguards that should be applied to the information systems: _____

This section is not required

****OPTIONAL Section D2 - Implementation of DIR 24 Recommended Security Procedures.**

Note: This section is OPTIONAL. Check here to include this section in the formal report.

In order to measure implementation of the DIR 24 recommended security procedures (available here) for information technology resources, please indicate if your department has developed security procedures in each of the 24 areas.

Note: if you choose not to implement any or all of the 24 procedures, you may want to document the risk management decision(s). Additionally, some procedures below are linked to the corresponding TAMU Standard Administrative Procedure as an example for universities.

Security Procedures Implementation	Implemented?
Acceptable Use - Please document any Risk Management Decision(s) here: _____	Yes No
Account Management - Please document any Risk Management Decision(s) here: _____	Yes No
Administrator / Special Access - Please document any Risk Management Decision(s) here: _____	Yes No
Authorized Software - Please document any Risk Management Decision(s) here: _____	Yes No
Backup Recovery - Please document any Risk Management Decision(s) here: _____	Yes No
Change Management - Please document any Risk Management Decision(s) here: _____	Yes No
Email Use - Please document any Risk Management Decision(s) here: _____	Yes No
Incident Management - Please document any Risk Management Decision(s) here: _____	Yes No
Internet / Intranet Use - Please document any Risk Management Decision(s) here: _____	Yes No
Intrusion Detection - Please document any Risk Management Decision(s) here: _____	Yes No
Network Access	Yes No

- Please document any Risk Management Decision(s) here: _____	
Network Configuration - Please document any Risk Management Decision(s) here: _____	Yes No
Password / Authentication - Please document any Risk Management Decision(s) here: _____	Yes No
Physical Access - Please document any Risk Management Decision(s) here: _____	Yes No
Portable Computing - Please document any Risk Management Decision(s) here: _____	Yes No
Privacy - Please document any Risk Management Decision(s) here: _____	Yes No
Security Monitoring - Please document any Risk Management Decision(s) here: _____	Yes No
Security Awareness and Training - Please document any Risk Management Decision(s) here: _____	Yes No
Server Hardening - Please document any Risk Management Decision(s) here: _____	Yes No
System Development and Acquisition - Please document any Risk Management Decision(s) here: _____	Yes No
Vendor Access - Please document any Risk Management Decision(s) here: _____	Yes No
Malicious Code - Please document any Risk Management Decision(s) here: _____	Yes No
Wireless Access - Please document any Risk Management Decision(s) here: _____	Yes No
Vulnerability Assessment - Please document any Risk Management Decision(s) here: _____	Yes No

This section will auto populate based on your previous answers.

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

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.

NOTE: Data entered is automatically saved when moving from field to field. Javascript is required.

FREQUENTLY ASKED QUESTIONS:

Before creating an account on ISAAC-S

Q: Do I have to use ISAAC-S?

A: If your TAMUS component uses information systems, yes. The State of Texas updated the security standards on November 24, 2004 and since TAMUS is a state agency, all components maintaining information systems must be in compliance with the state standards. ISAAC was originally created to assist Texas A&M University centers, departments, and colleges in meeting the state required security standards. ISAAC has been modified slightly so that TAMUS components having ownership or custodial responsibility for electronic information systems can ensure that on an annual basis, a security assessment report is completed.

Q: What is ISAAC-S?

A: ISAAC-S is a website that allows TAMUS components to register and perform a baseline security risk assessment of their information systems.

Q: What can I do through ISAAC-S?

A: You can:

Develop a Business Continuity/Disaster Recovery Plan for your information systems and data

Perform an automated, web-based Risk Analysis

Perform a Physical Security check of your premises

Find links to Security Awareness Training resources

Ensure compliance with state and local information security standards

Q: How much does an ISAAC-S account cost?

A: ISAAC-S access for TAMU System components is based on an annual subscription. Please see our pricing web site, or contact ITIM for details at (979) 845-9254.

Q: What type of equipment and software do I need?

A: You will need an Internet connection to access the ISAAC-S web site.

Acceptable web browsers are:

Netscape Navigator 4.05 or higher, with optimal performance at 4.6+

Microsoft Internet Explorer version 5.5 or higher, with optimal performance at 6.0+

Please note that the site is optimized for Internet Explorer and does require that you have JavaScript enabled and that your browser accept "cookies". If you need assistance with any of these settings, please contact ITIM at (979) 845-9254.

I have an ISAAC-S account - now what?

Q: How do I get started?

A: Once your IP addresses have been allowed to access the site, you can create an account online by clicking on "Create Account" button on the ISAAC-S login page. Also, you can call (979) 845-9254 and an ITIM Representative will be happy to assist you or answer any questions that you have concerning the ISAAC-S web site.

Q: What information do I need to begin?

A: You need to provide:

Information Systems Administrator contact information (phone, address, email, etc.)

Information Security Administrator contact information (phone, address, email, etc.)

Supervisory contact information (if one person is representing both functions above)

The automated Risk Assessment will require much more extensive information

Q: Can I choose my own user name and password?

A: Yes. But keep in mind that the UserID is limited to 8 characters, and the password must be at least 8 alpha / numeric characters (and no greater than 50 characters).

Q: Can I change my personal information and password?

A: Yes, ISAAC-S account holders are given the ability to change the personal information (such as: address, work phone, email, etc.) for the system and security administrators. You can change your password as long as you are able to login. If, however, you are unable to remember your password, a password reset is required, please contact an Information Technology Issues Management (ITIM) Representative at (979) 845-9254.

Q: What if I forget my UserID or password?

A: If you forget your UserID or password, you can request a new password by contacting an ITIM Representative at (979) 845-9254. We will email or phone the new password using the contact information in ISAAC-S.

How to Use ISAAC-S

Q: How can I view my departmental information?

A: From the Main Screen, you can preview and make changes to your departmental contact information.

Q: What happens to my data if the session times out?

A: If you lose connectivity to ISAAC-S unexpectedly, any data entered on a web form will be lost. The same is true if you leave your web browser inactive longer than 45 minutes. To avoid data loss, be sure to save your data by moving to another page.

Q: What if ISAAC-S goes down while I am using it?

A: If you lose connectivity to ISAAC-S unexpectedly, any data entered on a web form will be lost, but the changes which were made on any previous pages will be saved in the ISAAC-S database.