



ISAAC -The Information Security Awareness, Assessment, and Compliance System

The ISAAC web site was created to assist TAMU departmental information system representatives (e.g., system administrators) with assessing the security posture of their information systems, and measure compliance with information security standards (both state and local). Additionally, ITIM has created separate ISAAC applications for TAMU System components, Texas State Agencies, and University of Texas System components.

The ISAAC main status screen provides tools to meet compliance in the following areas:

- Business Continuity / Disaster Recovery Planning
- Risk Assessment
- HIPAA Module
- PCI Module
- Physical Security
- Security Awareness Training (TAMU only), and
- Resource Registration

TEXT SIZE
[A][A][A]

Business Continuity / Disaster Recovery Planning

The Business Continuity Planning module provides a guide for developing a business continuity and disaster recovery plan which will meet state and local information security standards. There is a detailed guide for departments with dedicated information technology staff and servers, and a simple plan for departments with a only desktop systems.

Risk Assessment

The Risk Assessment module provides an automated tool for both departmental servers and desktop systems. The risk assessment collects the following information: operational environment, asset valuation, in-place safeguards confirmation, and associated action plans for any shortcomings discovered. A full report can be generated once all requirements have been addressed.

HIPAA Module

The HIPAA compliance module was developed based on NIST Special Publication (SP) 800-66. The module addresses all HIPAA Security Rule standards and all associated implementation specifications, both required and addressable. Six of the standards include all the necessary instructions for implementation and have no associated implementation specifications.

PCI Module

The ISAAC tool provides a self-assessment module based on the PCI Data Security Standard. The PCI module is divided into six sections. Each section focuses on a specific area of security, based on the requirements included in the PCI Data Security Standard.

Physical Security

The Physical Security module provides a checklist which can be printed and used as a guide for making a visual inspection of the information systems host site.

Security Awareness Training

The Security Awareness Training module provides links to the TAMU Security Awareness Training certification web site, as well as other resources (including some sources for ordering free training materials - computer based training and video formats).

Resource Registration

The Resource Registration module provides a web form for identifying mission critical and/or confidential information resources. Additionally, the owners of the resources must be identified along with the custodians, and user base.

The ISAAC system has been upgraded and designated as version 2008 (7.0). In preparing ISAAC for the upcoming year several enhancements and improvements were implemented. In an effort to make sure that the risk assessment methodology maintains "best of breed" status, several risk assessment methodologies were reviewed and considered for enhancing the risk assessment module.