

**Automated Security Self-Evaluation Tools (ASSETs)**  
**Stanton S. Gatewood, Chief Information Security Officer**

University of Georgia  
Office of Information Security

## **Abstract**

*The University of Georgia's Internal Auditing Division and the Office of Information Security, utilizing existing internal staff, set out to complete the task of assessing 19 identified high-risk, highly visible and greatest target-of-opportunity operations on the University campus within about 100 days. Four of these units had experienced a significant security event in the previous year, and the others were deemed as susceptible. This analysis was followed by a broader effort to identify other units which house operations using sensitive data.*

*Considering the time sensitivity, limited resources, schedules and sheer number of departments and units, it became quickly obvious that the methodology and resources at hand would not suffice for the more than 350 colleges and departments which remained.*

*Conducting a qualitative risk assessment, IT identification/inventory and a compliance audit on remaining departments and units would not be effective, efficient or feasible. Therefore, in order to identify and manage at-risk IT systems effectively, a protocol was developed which placed the responsibility on the units themselves to perform and report self-evaluations: the Automated Security Self-Evaluation (ASSETs) program.*

## **Introduction of the Organization**

The University of Georgia, a land-grant and sea-grant institution, is the state's flagship institution of higher education and serves some 33,000 students. UGA is also the oldest, most comprehensive and most diversified institution of higher education in the state of Georgia, offering baccalaureate, master's, doctoral and professional degrees in a multitude of pursuits and attracting students from all parts of the world.

The University of Georgia Office of Information Security's (InfoSec) mission is to support the goals and objectives of the University of Georgia by assuring confidentiality, integrity and availability of its information and information systems, while also protecting instructional, academic and administrative systems. This is accomplished through the implementation of assurance methods that protect and defend these precious assets by:

- providing information security leadership;
- focusing on a reduction of the risk to systems;
- complying with applicable policies, laws and regulations;
- raising the awareness of the University community through training and education; and
- applying trusted technology.

UGA InfoSec offers the following core and essential services: Risk Management; Business Continuity and Disaster Recovery; Computer Incident Response Coordination; Security Awareness Training and Education; User and Endpoint Security; Secure Operations Center; and Policy Management.

## **Statement of Problem/Initiative**

The University of Georgia is a large Research-1 institution with a moderately sized IT unit responsible for its core network (backbone). The institution has more than 30,000 computer nodes in over 300 units. The IT support structure in the various units and departments is diverse, with different budgets, IT requirements, experience, priorities and cultures. Some units have full-time, trained IT staff, while other units rely on outside IT professionals (or have no IT staff at all). Each department/unit also brings a diversity of operating systems (Apple/Mac, Linux, MVS, Novell, UNIX, Windows, etc.), and it is difficult to be an expert on more than one platform. Often researchers are using computers funded by grants which have little or no provision for security measures or security maintenance.

Further complicating matters is the fact that each department/unit operates autonomously and independently of each other, with little impetus for inventorying, identifying and classifying sensitive or critical assets. The security stance of the units is reactive with no sense of shared responsibility.

In response to this challenging environment, the UGA Office of Information Security designed and developed an online database application, the Automated Security Self Evaluation Tools (ASSETs) program, which establishes a security baseline. The tools operate through a combination of hardware/software, secure processes and increased awareness. ASSETs' goals and objectives are to provide:

- Standardized Risk Assessment;
- Compliance Report Generator;
- Security Evaluation Report Generator;

- Security Plan Generator;
- Readily Available Security Tools; and
- Basic Business Continuity Plan Generator.

## **Design**

UGA InfoSec created an affiliation of campus IT and business personnel known as Unit Security Liaisons (USL). The USLs serve several strategic functions: 1) they allow UGA InfoSec to educate and empower an existing resource to implement the University's policies and procedures; 2) they increase knowledge at the academic or administrative unit level; and 3) they serve as InfoSec's point of contact for information security and compliance issues relating to that particular academic or administrative unit. To assist with implementation of the program, several hands-on lab classes were held, and a listserv was established to disseminate information.

The ASSETs program is 100% online, so all that is needed from a user's perspective is a computer with a browser (e.g., IE, Netscape, Firefox, etc.). With proper authentication credentials and an Internet connection, users can enter, view data or print reports from anywhere. The ASSETs program database allows additions, changes, deletions and updates by the authorized Unit Security Liaison at any time. In fact, the USLs are encouraged to add new equipment, delete equipment or change an answer to a question on the questionnaire.

Risk management is the ongoing process of identifying risks and implementing plans to address those risks. Often, the number of assets potentially at risk outweighs the

resources available to manage them. It is therefore extremely important to know where to apply available resources in order to mitigate risk in a cost-effective and efficient manner.

Conducting a university-wide qualitative risk assessment is a process that requires a strong commitment from senior management as well as collaboration between cross-functional colleges/departments. Assessing information risks is a management issue, not a technology issue; therefore, to be most effective, the process should be considered a shared responsibility with accountability resting with all members of management and the institution.

Risk assessments should be considered an ongoing process, not a one-time project. The ASSETs program consists of a set of steps that are repeated on an ongoing basis. Steps 1 – 5 are to be completed in the first year, and Step 6 follows in the second year. The steps are as follows:

1. Inventory Assessment

In assessing information technology security risks for a college/department, the first step is to inventory all critical and sensitive servers to determine the scope of the risk. This process identifies the physical and information assets that constitute the college/department. Characterizing the college/department and IT system provides information (e.g., hardware, software, system connectivity and sensitive/critical information) vital to defining the risk. Such an inventory assessment is essential to the UGA InfoSec's philosophy: *"You can't secure an asset if you don't know it exists."*

## 2. Risk Assessment/Classification/Valuation/Tools

A simple qualitative risk assessment will assign a rating of high, medium and low for probability and impact for the critical and sensitive server issues identified in Step 1. Security tools regarding policies/secure processes, technology and awareness are available online – all in one location.

## 3. Security and Business Processes Questionnaire

A questionnaire assists college/department security liaisons in evaluating security processes and procedures in order to promote the protection and security of information assets and resources. The goal is to provide a comprehensive approach to enhance security within the college/department by presenting opportunities to mitigate risk.

## 4. Security Evaluation Report

The evaluation provides information on the existing measures the college/department has in place relative to security.

## 5. Security Plan

The goal of the security plan is to determine an appropriate level of security and arrange to organize suitable security for the college/department IT assets. Every college/department is expected to develop and maintain a security plan. The risk assessment helped determine the college/department's IT security risk level; the security questionnaire helped evaluate the college/department's IT security strengths and weaknesses; and now an IT security plan for the college/department can be developed.

## 6. College/Department-Level Baseline Business Continuity Plan (BCP)

Once Steps 1 – 5 are completed, the user may then produce a customized unit-level Business Continuity Plan (BCP). The data from the previous steps are imported into a BCP developer application to create this vital document.

### **Implementation**

The most important aspect of implementation is the realization of a sense of urgency. You must start your efforts now and not wait for a security incident to dictate your response. The steps to successful implementation may be outlined as follows:

1. Obtain the support of senior management.
2. Inventory all existing security policies.
3. Inventory all existing security technology.
4. Create supporting policies, if necessary.
5. Research all “risk management” standards, best practices and methodologies.
6. Research current business processes.
7. Select appropriate methodology for your environment.
8. Create a statement of goals and objectives.
9. Tie all goals and objectives to the institution’s business goals and objectives.
10. Create a strategy to reach the goals and objectives.
11. Develop awareness material.
12. Assemble project teams.
13. Present the project plan.
14. Set deliverables and timelines.

15. Check regularly.
16. Proceed to Step #1 of ASSETs . . .

Implementation timelines: You should plan on completing Steps 1 – 5 of the ASSETs program in the first year and Step 6 in year two.

### **Benefits**

UGA ASSETs provides a comprehensive set of online, intuitive, extensible and automated tools for college and department security liaisons. These tools include self-assessment, security, compliance reporting and security planning for the unit’s own assets, as well as self-help and “shared responsibility” for information and information systems security.

#### UGA ASSETS:

- takes a practical, standards-based approach to risk assessment without undue complexity;
- determines appropriate protections for university systems and information;
- aids in achieving compliance;
- identifies risk and focuses mitigation efforts on sensitive systems and significant vulnerabilities;
- helps avoid devoting resources to mitigating low-risk vulnerabilities;
- scales testing efforts to the sensitivity of a system and its risk level;
- provides an “IT risk assessment standard.”

Additionally, ASSETs:

- follows the NIST 800-26 Security Self Assessment Guide for Information Technology Systems;
- provides a general understanding of the overall health of the department or unit security program;
- offers recommendations for needed security improvements;
- fulfills reporting requirements, identifies resources, and helps prepare audit information; and
- assists in preparing and submitting budget requests.

The ASSETs program requires no additional financial investment by the University of Georgia. Its tools are available through shareware or freeware, and the institution uses its existing InfoSec technology investment. The questionnaires and checklist are extensible to allow for customization and enhancement.

### **Retrospect**

ASSETs is proving to be just that – a valuable asset to the University of Georgia’s IT security effort. In retrospect, our only regret is that we did not begin the program sooner.