

2009 Information Security Risk Assessment Overview

What?

Information security risk assessment involves identifying and assessing risks to confidentiality, integrity and availability of information and information systems. A typical self-assessment involves an extensive questionnaire with defined control objectives and techniques derived from requirements and best practices found in statute, policy and guidance on information security. The process measures information systems against these requirements and identifies gaps in meeting them. Repeat assessments measure progress toward them. The Information Security Office will facilitate a risk assessment in academic and business units throughout the University during Summer 2009.

Why?

A risk assessment is a prerequisite to the formation of strategies for developing, implementing and maintaining an information security posture. The ABOR Audit Committee requested UA to conduct a risk assessment. The need for risk assessment is emphasized by:

- ABOR Policy 9-202
- ABOR Information Security Program Guidelines
- Risk Assessment Standard
- State Office of the Auditor General Performance Audit Report
- HIPAA, for both covered entities and business associates
- Certain grants and governmental partnerships

Who?

- *Information Security Office* prepares and distributes documentation, trains ISLs, prepares reports
- *Academic and administrative departments* perform risk assessment and prepare action plans
- *Internal Audit* reviews departmental progress

How?

- Risk Assessment Procedure (see reverse)
- Excel spreadsheet
 - Instructions and identifying information
 - Central application and data inventory
 - Unit application and data inventory
 - Hardware inventory
 - Business risk profile
 - Security assessment questionnaire
 - Signatures
- List of optional inventory tools
- Action Plan form
 - Executive summary
 - Decision support worksheet, with cost-benefit analysis tool

When?

- Beginning on or after July 1, 2009
- Return to UIISO by August 31, 2009

Where?

- <http://security.arizona.edu/risk>

Information Security Risk Assessment

