IT RISK ASSESSMENT PROCEDURE

Arizona State University is committed to continually improving information technology in accordance with business needs, industry standards, best practices and legal requirements. We regularly review and rank our risks so we can mitigate risk proactively. This document outlines our approach for identifying and analyzing risk areas and taking corrective action in an effort to provide the most strategic, available and secure IT environment possible.

Scope

This document describes the process for conducting IT Risk Assessments at ASU. Both centralized and decentralized functions are reviewed periodically. ASU's IT Risk Assessment cycle is a continuous improvement plan for assisting the business units with implementing University information security guidelines. The cycle is outlined as follows:

1. Identify areas of IT risk across the University.
2. Identify corrective measures to be taken.
3. Follow-up review of corrective measure implementation.
4. Enforcement of corrective action measures where necessary.

ASU conducts IT risks assessments periodically. This document defines each key role in the assessment process along with procedural guidelines for:

- developing the Risk Assessment
- distributing the survey
- analyzing and distributing responses
- developing and conducting the corrective action plan

Roles

Information Security Office

ASU's Information Security Office (ISO) develops, maintains, and conducts the Risk Assessments. This office also analyzes and disseminates the results.

Executive Leadership

ISO works with the Information Security Task Force and other ASU management, as appropriate, to identify both the appropriate survey respondents for each department (business unit) and a corrective action working group. This group provides communication and endorsement of the IT Risk Assessment process to the business units.

Corrective Action Workgroup

The Corrective Action Workgroup addresses the top risk areas across the University. This workgroup reviews those items requiring additional action; identifies University-wide or departmental accountability and corrective actions to be taken; and identifies areas to be addressed with consultation, documentation, presentations, or training materials. Constitution of the Corrective Action Workgroup may vary depending on the risk areas identified in a given Risk Assessment.

IT Risk Assessment Survey Respondents

The IT Risk Assessment survey respondents are department liaisons designated by the appropriate dean or Department Head. Assessments are conducted using a survey distributed to departments University-wide.

Survey mechanism
Survey questions are derived from industry standards including ISO/IEC 17799:2005, COBIT 4.1, COSO, and NIST 800-30. The questionnaire may include open-ended questions for respondent feedback on the survey mechanism and issues not covered in the multiple-choice questions.

Review of survey questions
Survey questions are reviewed before distribution to gauge their effectiveness and identify the range of possible responses to each question. The Information Security Office will assign appropriate ratings for each possible response.

The review process may include facilitated small group discussions, presentations with extended Q&A sessions, and/or requests for feedback by electronic mail. The survey typically emphasizes questions that were indicated as high risk areas University-wide in previous assessments. The survey will include benchmarks, as appropriate, with other universities undertaking similar efforts.

Distribution

Business Units and Respondents
The survey is distributed to all high level academic and administrative units of the University. The ranking IT and business administrators are the survey respondents for their unit. The survey is distributed electronically and will include the endorsement of senior management.

Publicity
Prior to distribution of the survey, the Risk Assessment will be communicated to all units involved and to senior University management. The Risk Assessment process should be announced from senior management to their respective department(s).

Analysis and dissemination of results
The Risk Assessment is analyzed at the departmental level and University-wide. The Information Security Office computes the Impact, Likelihood, Combined Risk Value, and Risk Rating for the response to each question.

For each survey returned, the ISO summarizes the results and provides an overview of risk areas that require varying degrees of remediation.

Results are disseminated in management letters to department heads and reported to the University executive leadership and the Corrective Action Planning Workgroup.

Corrective action
The top risk areas identified in the Risk Assessment results are addressed through a University Corrective Action Plan developed in response to the aggregate Risk Assessment results. Each Corrective Action Plan has its own timeline to allow adequate time for departmental implementation before the follow-up Risk Assessment. General guidelines are given here.

Convene Corrective Action Workgroup
On review of the Risk Assessment results, the Information Security Office convenes the Corrective Action Workgroup and presents the findings. Depending on the findings, members may be added to the group to address specific knowledge or expertise.

Develop Corrective Action Plan
The Corrective Action Workgroup reviews the top risk areas and develops a plan to address those areas University-wide. A range of possible corrective actions are identified, including:
- information security training for university personnel
- presentations or training materials tailored to specific departmental needs
- provision, improvement, and/or documentation of centralized services and resources
- model processes for business units to follow or adapt as appropriate
- consultation with business units to identify existing resources and develop appropriate departmental corrective action plans

**Pilot Corrective Action**
Where necessary, the Corrective Action Plan is implemented in a pilot business unit. The pilot business unit works closely with the Information Security Office to apply appropriate corrective actions and provides feedback to the Corrective Action Planning Workgroup on key elements of the plan. This allows for testing and fine-tuning of the Corrective Action Plan before rollout to all applicable business units.

**Conduct Corrective Action Plan**
After any pilot actions are completed, the Corrective Action Plan is made available and publicized to all appropriate business units for departmental implementation. The plan should be communicated and promoted in a variety of ways; recommended communication mechanisms include:
- publication on the Information Security Office’s Web site, getprotected.asu.edu
- orientation sessions presented in person to business unit representatives
- electronic mail from senior management including endorsement of the process

**Enforcement**
Each business unit is responsible for taking corrective action based on its Risk Assessment results and the Corrective Action Plan. The effectiveness of University and departmental corrective actions is measured in subsequent Risk Assessments. The Risk Assessment Team, including the University Technology Office, the Information Security Office and the Corrective Action Workgroup may escalate any issues or concerns through the appropriate management channels up to the executive level.