Internal Risk Assessments and Corrective Action Planning

IT Decentralized Risk Assessment
Corrective Action Planning Workgroup
February, 2010
Objectives

• Put the risk assessments in context
• Lay out the timeline for corrective actions
• Identify corrective action planning resources
• Provide a general “road map”
Background

- Risk assessments conducted 2009
  - By University Audit & Advisory Services
    - Q2 2009: Decentralized IT Risk Assessment
    - Q3 2009: Centralized IT Risk Assessment
  - Reported to ABOR
  - Referenced in report to Auditor General’s Office
Auditor General’s Office said…

- According to officials, the university intends to monitor compliance with the information security program through its risk assessments. In fiscal year 2009 the university’s [University] Audit and Advisory Services completed two risk assessments, however ASU is still developing a plan for monitoring information security program compliance, including mechanisms for responding to noncompliance and holding departments accountable.
ASU proposed...

- Decentralized
  - University-wide training, departmental outreach
- Schedule
  - Initial Risk Assessment – Q2 2009
  - Evaluate/Develop Corrective Action Plan – Q4 2009
  - Conduct Corrective Action Plan – 12/2009 through Q1 2010
  - Follow-up Risk Assessment – Q2 2010
  - Evaluate/Develop Corrective Action Plan – Q4 2010
ASU proposed...

• Centralized
  – Follows the same model
  – Schedule
    • Initial Risk Assessment – Q3 2009
    • Evaluate/Develop Corrective Action Plan – Q1 2010
    • Conduct Corrective Action Plan – Q2 2010
    • Follow-up Risk Assessment – Q3 2010
    • Evaluate/Develop Corrective Action Plan – Q4 2010
Decentralized risk assessment

• DRA summarized 20 points of concern
  – Units differ in points to be addressed
  – Each unit may require its own plan

• ASU has…
  – Convened a working group
    • Reviewed items requiring additional action
    • Identified ASU-wide/departmental corrective actions
    • Identified areas where UTO can assist
    • Finalized the corrective action plan
  – Developed security awareness training
    • For faculty/staff/employed students
    • Addresses most of the 20 points
    • Available through Blackboard now
  – Drafted a guide for unit responses
The road map

• Review your survey responses
  – 1, 5, 8, 10, 18-19, 21, 23-25, 27-28, 31-32, 35, 37-38, 47, 49-50, 64, 68
  – Scores of 4 or 5
• Refer to the CAP guide
  – http://getprotected.asu.edu/capguide
• Walkthrough – your survey
  – If you have more than one, just pick one
The road map

• Promote the GISA training to your personnel
  – Details: http://help.asu.edu/Security_Awareness
  – Include topic reinforcements in announcement

• Coordinate with UTO where needed
  – Web application scanning
  – Disaster Recovery plans
  – Potentially useful centralized services
  – Service Desk (feedback survey)

• Draft departmental documentation if needed
  – Business Continuity plan
  – Incident Response procedures
The road map

- **Timeline**
  - February: Training, planning, resource gathering
  - March: Completion
  - April: Follow-up risk assessments
Questions?

infosec@asu.edu