

2009 Information Security Risk Assessment Action Plan Instructions

This page includes instructions for completing the Action Plan referred to in Steps 6, 7 and 8 of the Risk Assessment Procedure, <http://security.arizona.edu/files/ISP1200.pdf>.

1. *Insert identifying information on page 1.* The first page of the Action Plan (following the instructions) will inform your unit's senior administrator of the Action Plan's purpose. On page 1, insert:
 - a. Unit Name
 - b. Months
 - c. Name of Senior Financial Administrator
 - d. Name of Senior IT Administrator

2. *Complete Decision Support Worksheets.* The 2009 Information Security Risk Assessment Report delivered to your unit by the University Information Security Office includes recommended controls for significant risks identified in the assessment process. Controls are organizational, procedural or technological means of managing risks. Step 7 of the Risk Assessment Procedure tasks the assessment team with developing an Action Plan for the "High Priority" recommendations. The template following these instructions incorporates analytical tools, including a formal cost-benefit analysis, to support the assessment team's decisions. The cost-benefit analysis provides a consistent, comprehensive structure for identifying, scoping and selecting the most effective and cost-efficient mitigation solution. A sample completed cost-benefit analysis form appears on the next page.

Complete Decision Support Worksheets for –

- each high priority recommendation in the Report
- any alternative control that may be effective at mitigating the risk addressed by a high priority recommendation (see <http://security.arizona.edu/files/controls.pdf> for a list of controls)
- additional "Medium Priority" recommendations or "Low Priority" recommendations you choose to consider

If the assessment team decides to consider more than one control for a single recommendation, develop a Decision Support Worksheet for each, then compare the results before selecting a risk mitigation strategy.

Analytical tools such as risk assessment and cost-benefit analysis impart insight and discipline to the decision-making process. They can aid in identifying and evaluating options, and, perhaps, achieving greater benefits at less cost. However, these tools are not substitutes for human judgment. For example, the assessment team may believe a particular recommendation is not identified as high priority in the report because it has not been given sufficient weight. In that case, the team should consider completing a Decision Support Worksheet for the risk. Please contact the Information Security Office if you need assistance in identifying a security control for any such risk. Another example would be when the cost and/or benefit proves difficult to quantify or qualify.

3. *Delete this instruction page and the sample cost-benefit analysis table following this page.*

4. *Submit the Action Plan to your unit's senior administrator.*

REMOVE THIS PAGE BEFORE SUBMITTING THE ACTION PLAN TO YOUR UNIT'S SENIOR ADMINISTRATOR

Sample Cost Estimate for Implementing Smart Cards for VPN and Admin Access

Category	Notes	Estimates
Acquisition costs for hardware, software and services	Cost is \$15 per smart card and \$15 per reader. 100 employees require VPN or administrative access. The total cost for cards (\$15 x 100) and readers (\$15 x 100) is \$3,000.	\$3,000
Implementation costs	Consultant at a cost of \$20,000. IT staff would invest 40 hours.	\$20,000 40 hours
Management, monitoring and maintenance costs	See "Costs of auditing and verifying effectiveness"	--
Costs of communicating new policies & procedures	Use established means of communicating news to employees, such as e-mail newsletters, internal Web sites, and e-mail mailing lists	4 hours
Training costs for IT staff	Same consultant would train IT staff at no additional cost. IT staff would miss 4 hours of work time.	4 hours
Training costs for users	Web-based training included in the cost of hardware. 100 employees would invest 1 hour each.	100 hours
Costs to productivity and convenience	Assume average user will miss 1 hour of productivity, 100 hours total. Assume one out of four will call 24/7 IT Support Desk for help with their smart cards, at an average of 10 minutes per call for each user and support staff member, approximately 80 hours.	180 hours
Costs of auditing and verifying effectiveness	IT staff can periodically audit and verify the effectiveness of the new control.	20 hours/year
Total	\$, hours and other costs	\$23,000 328 hours initially 20 hrs/yr ongoing

**2009 Information Security Risk Assessment
Action Plan
Unit Name: _____**

Executive Summary

The Risk Assessment Standard, <http://security.arizona.edu/files/ISS1200.pdf>, requires each unit to conduct an information security risk assessment every three years. To comply with this requirement, the unit formed a team to perform an assessment of the unit’s information assets. The risk assessment was conducted during _____, 2009, in accordance with the Risk Assessment Procedure, <http://security.arizona.edu/files/ISP1200.pdf>.

After the risk assessment documentation was submitted to the Information Security Office, the team received a report summarizing findings and recommendations. The report identifies certain high priority recommendations for the most significant risks identified in the assessment process. This Action Plan recommends actions to mitigate the high priority recommendations.

Recommended Mitigation Strategies

The team completed a Decision Support Worksheet for each high priority recommendation. The worksheets are included in this Action Plan. Each worksheet provides a consistent, comprehensive structure for identifying, scoping and selecting the most effective and cost-efficient mitigation strategies for the identified risks.

The team recommends the actions detailed in the Decision Support Worksheets.

Requested Action

Please review this Action Plan and indicate your approval or rejection below. Please do not hesitate to contact the following team members for clarification, as needed:

Senior Financial Administrator: _____
Senior IT Administrator: _____

If you approve the Action Plan, please submit copies of the Action Plan to the unit’s Vice President or Dean and the University Information Security Officer. If you reject the Action Plan, please return it to the assessment team. Thank you for your consideration.

Approved: Name: _____ Signature: _____ Title: _____ Date: _____	Rejected: Name: _____ Signature: _____ Title: _____ Date: _____
---	---

Decision Support Worksheet

1. Identify a risk and its control solution:
 - Copy a Recommendation from the Report
 - Describe an alternative control

2. Indicate the level of priority assigned to the Recommendation in the Report. (This is the level of the **risk** referred to below in step 3.)
 - High (for High Priority recommendations)
 - Medium (for Medium Priority recommendations)
 - Low (for Low Priority recommendations or recommendations without a priority designation)

3. From step 1 above, review the control solution and determine how effective it is in reducing the risk:
 - Highly effective in reducing the risk
 - Average in reducing the risk
 - Poor in reducing the risk

This is the **benefit** of the control solution.

4. Estimate the **cost** of the control solution. Some costs may be quantified in hours or dollars. Others, such as costs to productivity and convenience, may be qualified as high, medium or low rather than quantified. Rough estimates are sufficient but should not replace any project justification process your unit requires. The table may be modified.

Category	Notes	Estimates
Acquisition costs for hardware, software and services		\$
Implementation costs		\$
Management, monitoring and maintenance costs		\$
Costs of communicating new policies & procedures		\$
Training costs for IT staff		\$
Training costs for users		\$

Costs to productivity and convenience		<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
Costs of auditing and verifying effectiveness		\$
Total	\$, hours and other costs	\$

5. Determine whether the estimated cost (from step 4) is reasonable relative to the degree of risk reduction possible with the control solution (from step 3):

- Yes, because _____
- No, because _____

6. Select a risk mitigation strategy:

- Mitigate by accepting the Recommendation
- Reduce the risk by selecting another control solution (for which a separate Decision Support Worksheet has been included in the Action Plan)
- Transfer the risk by outsourcing the function to a partner or vendor that agrees to assume responsibility for mitigating the risk
- Accept the risk and continue operating
 - Often the best choice when:
 - the cost of the control is too high relative to the degree of risk reduction possible with the control solution
 - the impact of the control on the unit's ability to do business is too high relative to the value of the asset needing protection
 - Not an option for a control mandated by law.
 - Not an option for a control mandated by university policy or standards unless an exception is obtained from the University Information Security Officer.

7. Summarize the reason for selecting the risk mitigation strategy in step 6. Attach any additional project justification documentation required by unit's procedures or guidelines.

8. Establish a target date(s) for implementation, if applicable: _____

9. Name personnel responsible for implementation, if applicable: