Goal and scope:
The Web Application Security Review will assess whether security requirements and controls are functioning effectively, as well as remediate, based on risk, problems identified during the review program. Security reviews include a university-wide security review program and an ISO partnership review program.

**University-wide security review program:** All departments are responsible for following the university-wide security program.

**Year One:**
1. Complete security risk assessment, updating application inventory and *data* classification
2. Develop and implement action plans as needed to address vulnerabilities, using application inventory, *data* classification and risk assessment vulnerability report.
3. Run *network* and application scans for systems containing web applications

**Year Two and Three:**
1. Run *network* (IS-P601) and application (IS-P801) scans to verify effectiveness of remediation and controls
2. Address any further remediation as indicated by *scans*

**ISO partnership security review program:**
The ISO will work in partnership with a portfolio of departments during each security review program cycle.

**ISO partnership selection:**
Information from the risk assessment will be used to select the departments for the ISO security review partnership.

**Procedure**
1. The ISO will provide assistance by working with the technical team of the department as needed to develop and clarify the focus of the risk assessment action plan. The action plan should be guided by *data* from the application inventory, *data* classification and risk assessment vulnerability report. The department may receive advice or choose to run initial *network* and/or application *scans* to gather specific *data* for remediation steps. The action plan will include remediation actions and/or security controls, depending on the nature of the vulnerability and the resource required for remediation, timelines for each action item, and checkpoints for reporting and monitoring overall plan progress.

2. The ISO will meet with the department head and technical team to make any final adjustments and approve the action plan.

3. The ISO will meet with the department to discuss progress reports and to provide advice and guidance at defined checkpoints to help ensure success in enacting the action plan.

4. *Network* and application scanning tools will be used semi-annually during the program to provide metrics on the security environment to the department and ISO.
**Related Guidance**
Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Exceptions Procedure (IS-P100)
Data Classification Standard (IS-S302)
Application Security Standard (IS-S801)
Web Application Security Assessment Procedure (IS-P801)
Risk Assessment Standard (IS-S1200)
Risk Assessment Procedure (IS-P1200)

All *italicized terms* used in this standard are defined in the Information Security Terms Guideline (IS-G100).

**Revision History**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft</td>
<td>08/03/10</td>
</tr>
<tr>
<td>UA-ISAC Review of Initial Draft</td>
<td>08/16/10</td>
</tr>
<tr>
<td>Sent to UA-ISAC for review after revision</td>
<td>08/23/10</td>
</tr>
<tr>
<td>Effective Date</td>
<td>08/23/10</td>
</tr>
</tbody>
</table>