What is a security risk assessment?
An 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.

In 2009/2010, the Information Security Office facilitated a security risk assessment in academic and business units throughout the University. The University of Arizona is required to repeat such an assessment every three years.

What has changed from the last risk assessment?
The previous assessment was delivered to campus units in a seven-part Excel workbook. Three of the seven parts to the assessment contained inventory items (hardware, central software inventory and unit software inventory). Two additional parts were instructions and an attestation page. The remaining two parts were the Business Risk Profile (BRP) and the Security Risk Assessment (SRA). These two parts will be delivered to units online via SharePoint, and can be completed this way. Following is an explanation of what is contained in these two parts:

1. **Business Risk Profile** (BRP): In the normal course of doing business, organizations regularly make certain technical and business decisions that could introduce security risks that need to be mitigated. The BRP helps identify which of those risks your unit faces and provides a baseline against which to compare the measure of Defense-in-Depth (DiD). The questions cover the following areas:
   a. Basic Information (4 questions)
   b. Infrastructure Security (min 8 questions; max 11 questions)
   c. Application Security (min 10 questions; max 11 questions)
   d. Operations Security (min 11 questions; max 13 questions)
   e. People Security (min 8 questions; max 9 questions)
   f. Compliance Areas (11 questions)
   o **BRP # of questions:**
     - Minimum: 52
     - Maximum: 59

2. **Security Risk Assessment** (SRA): The SRA helps identify security measures deployed within your unit to mitigate risks identified in the BRP. The questions cover the following areas:
   a. Infrastructure Security-Perimeter Defense (min 8 questions; max 26 questions)
   b. Infrastructure Security-Authentication (14 questions)
   c. Infrastructure Security-Management and Monitoring (min 12 questions; max 16 questions)
   d. Application Security-Deployment and Use (min 11 questions; max 17 questions)
   e. Application Security-Application Design (min 4 questions; max 7 questions)
f. Application Security-Data Storage and Communications (2 questions)
g. Operations Security-Environment (min 6 questions; max 10 questions)
h. Operations Security-Security Policy (min 6 questions; max 10 questions)
i. Operations Security-Patch and Update Management (min 5 questions; max 13 questions)
j. Operations Security-Backup and Recovery (min 2 questions; max 6 questions)
k. People Security-Requirements and Assessments (min 3 questions; max 11 questions)
l. People Security-Policy and Procedures (min 3 questions; max 5 questions)
m. People Security-Training and Awareness (min 2 questions; max 6 questions)

**SRA # of questions:**
- Minimum: 97
- Maximum: 143

---

**Instructions for Completing Risk Assessment**
Step-by-step instructions can be found on page 3 of this document. The instructions include directions for accessing the final documents on the SharePoint site.

---

**Resources**
- Information Security Office SharePoint Site
- SharePoint Business Risk Profile
- SharePoint Security Risk Assessment

**Related Guidance**
- Information Security Policy (IS-100)
- Information Security Terms Guideline (IS-G100)
- Exceptions Procedure (IS-P100)
- SSN Usage Standard (IS-S301)
- Data Classification Standard (IS-S302)
- Risk Assessment Standard (IS-S1200)
- 45 CFR 164.308(a)(1)(ii)(B) [HIPAA]
- 16 CFR Part 314, Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act]

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

**Revision History**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft</td>
<td>05/06/09</td>
</tr>
<tr>
<td>Effective Date, v1</td>
<td>07/01/09</td>
</tr>
<tr>
<td>Revision Date</td>
<td>1/7/13</td>
</tr>
<tr>
<td>Effective Date, v2</td>
<td>1/24/13</td>
</tr>
<tr>
<td>Effective Date, v3</td>
<td>1/27/13</td>
</tr>
</tbody>
</table>
Step-by-Step Instructions

Risk assessments are vital processes for maintaining the security of university resources and meeting legal requirements for protecting confidential university data. This procedure defines a process, roles and responsibilities for the periodic risk assessment mandated by the Risk Assessment Standard (IS-S1200).

The Vice President, Dean, Director, Department Head, Head of Center or other senior administrator of a unit is referred to in this procedure as the unit head.

Documentation and resources referred to in this procedure can be accessed on the Standards, Procedures and Guidelines page at http://security.arizona.edu. Word, Excel and Portable Document Format (pdf) versions of the risk assessment are available as working copies for the assessment team’s use. The Information Security Office’s (ISO’s) SharePoint site is the official data gathering resource for submitting each unit’s risk assessment to the UISO.

The risk assessment completion process is presented below. A flowchart of the procedure appears on the final page.

I. Assessment Team
   A. Each unit head is to designate an Information Security Liaison (ISL) for the unit and inform the University Information Security Officer (UISO), as stated in the University Information Security Policy (IS-100). The ISL will serve as the driver behind the process for the unit and as the primary point of contact for the ISO.
   B. The unit head will assist the ISL, if necessary, with the organization of the assessment team. Assessment team members should be knowledgeable of their unit’s infrastructure, applications, operations, policies and procedures, and dependence on central systems and operations. At a minimum, the team should consist of the unit’s ISL, the senior IT administrator, and the senior financial administrator (The ISL may also serve in one of these positions).
II. Assessment Team Planning and Working Copy Completion
   A. The unit ISL should schedule and convene a session for the assessment team in order to plan completion of the two parts of the risk assessment: the Business Risk Profile and the Security Risk Assessment.
      i. Prior to convening the meeting, send working copies of both parts of the risk assessment to your team. Working copies are available in Word, Excel and PDF formats, and are available for download on the Information Security website.
   B. If appropriate, assign members of the team to complete different portions of the Business Risk Profile and Security Risk Assessment, according to team members’ core competencies.
   C. Schedule additional sessions, if necessary, to reconvene and complete the working copies prior to completing final version of the risk assessment for submission to the ISO.
   D. Provide completed working copies of the BRP and SRA to your Department Head for feedback and approval before completing the online assessments.

III. Online Assessment Completion
   A. All ISLs have been given access to complete the Business Risk Profile and Security Risk Assessment on the Information Security Office’s SharePoint site by use of UA NetID and Password.
      i. If units intend to have another team member who is not the unit ISL complete the assessments on SharePoint, please contact the Information Security Office at infosec@email.arizona.edu. In the communication, include the name and UA NetID of the assessment team member who needs access to SharePoint site.
      Because of the confidential nature of a risk assessment, only the Information Security Office and the employee completing the assessment documents on SharePoint will be able to access the documents.
   B. When you are ready to complete the BRP and SRA, click on the appropriate link and follow these instructions for filling out the webform:
      i. Click on BRP or SRA
      ii. You will be brought to a login page. Use your UA NetID and Password to log into the SharePoint site.

NOTE: You will be logging in to Catnet, so make sure that “CATNET\” is typed in front of your NetID.
iii. You will be brought to a SharePoint menu screen where you can create a new "Item." The BRP screen will look like this:

iv. Click on "New," and you will be able to create a "new list item."

v. Use your working copy to assist you in responding to all questions in the appropriate online questionnaire.

vi. When you reach the end of each questionnaire, you can choose "in process" or "completed" from the dropdown menu. If you think you will need to go back to verify answers or enter additional information, select "in process." If you are sure you are done, select "completed." Then click "OK." This will save your questionnaire.
vii. NOTE: If you are going to return to finish one of both questionnaires at a later time, you will click the “Edit” image beside the item you created earlier.

C. When both the Business Risk Profile and the Security Risk Assessment are completed in the SharePoint form, the ISL should send an email the ISO (infosec@email.arizona.edu), with the unit head carbon copied in the email, confirming that both parts of the risk assessment (BRP and SRA) have been completed and submitted online. Use this language as the template for your confirmation email:

“On behalf of [DEPARTMENT(s)], I certify that our department has completed the 2013 Security Risk Assessment in the Online Forms provided at the ISO SharePoint site. [DEPARTMENT HEAD(s) NAME(s)] has (have) reviewed copies of the Business Risk Profile and Security Risk Assessment documents and has (have) approved these documents as final.”

This email serves as a formal certification of completion by the unit’s assessment team.

Working Sessions with ISO Staff
The Information Security Office Staff will hold several “clinics” to assist units that may not have dedicated IT staff, or who may have questions where assessment teams need clarification. All Sessions will be held in the Computer Center, 1077 N. Highland Ave., Room 116 from 2:00-4:00 pm. The dates for the sessions are as follows:

- Feb. 5, 11, 19, 26
- March 5, 12, 26
- April 2, 9, 16, 23