



Department of Information Resources

SPECTRIM **Risk Assessment** **Guide**

Contents

| | |
|---|----|
| 2.0 Roles | 4 |
| 3.0 Risk Assessment Activity Summaries..... | 5 |
| 4.0 Logging into SPECTRIM..... | 7 |
| 5.0 Scoping the Assessment..... | 8 |
| Activity 1 – Create Risk Assessable Unit (RAU)..... | 8 |
| Activity 2: Create Risk Assessment Components..... | 13 |
| Activity 2a: Create an Application Risk Assessment Component | 13 |
| Activity 2b: Create a Location Risk Assessment Component..... | 19 |
| Activity 2c: Create a Network Risk Assessment Component..... | 23 |
| Activity 3: Generate the Assessment Questionnaires | 26 |
| Activity 3a: Create an Application Assessment | 26 |
| Activity 3b: Create a Location Assessment..... | 31 |
| Activity 3c: Create a Network Assessment | 36 |
| Activity 3d: Create an Organization Security Program Assessment | 41 |
| 6.0 Launching the Assessment | 46 |
| Activity 4: Save the Risk Assessable Unit and Initiate Assessment Workflow..... | 46 |
| 7.0 Completing the Assessment | 47 |
| Activity 5: Complete the Assessment Questionnaire | 47 |
| 8.0 Reviewing the Assessment | 50 |
| Activity 6: Approve or Reject the Questionnaire..... | 50 |
| Activity 7: Approve or Reject the Questionnaire..... | 53 |
| 9.0 Responding to Findings | 56 |
| Activity 8: Respond to Findings | 56 |
| Activity 9: Approve or Reject Finding Submission | 63 |
| Activity 10: Forward Completed RAU to ISO for Approval | 65 |
| 10.0 Approving the Risk Assessable Unit..... | 66 |
| Activity 11: Approve or Reject the RAU..... | 66 |
| Activity 12: Approve or Reject the RAU..... | 68 |

1.0 Definitions

Risk Assessable Unit (RAU) – The scope of a risk assessment. The RAU is what is being assessed. It may be a department, an application, a location such as a data center, or groups of homogeneous hardware (windows servers, laptops, etc.).

Assessment component – Each piece that makes up the RAU. For example, if the RAU is the Student Information System (SIS), the assessment components might include the SIS application, SIS databases, the SIS location, and network infrastructure.

Integrated Control Framework (ICF) – The basis for determining which controls to assess (based on the criticality of the information resource) and for creating the assessment questionnaires. The ICF incorporates the information security controls and enhancements from [NIST SP 800-53v4](#).

Assessment questionnaire – The list of information security questions asked during an assessment. Each question relates to one or more of the security requirements contained in the ICF. Each assessment component has its own questionnaire.

2.0 Roles

Risk Assessment Coordinator

The Risk Assessment Coordinator (RAC) is responsible for determining the scope of the risk assessment, identifying the components of the risk assessment, and determining who will complete and review the assessments. The RAC shepherds the assessment process from planning to conclusion. Organizations can have one or multiple RACs, normally a member of the Information Security Officer (ISO) staff. The RAC will create the RAU, add relevant assessment components, generate the questionnaire for each component, and track assessment progress.

Information Security Officer

The Information Security Officer (ISO) is normally the final approver of a risk assessment. This is the designated individual with overall responsibility for the RAU. The ISO is responsible for reviewing the appropriateness and accuracy of the assessment and all related findings (i.e., may review the results of all the assessment questionnaires that make up the RAU).

Assessor

The Assessor is responsible for completing the assessment questionnaire. For each assessment component, the Assessor must complete an assessment questionnaire. When all questions have been answered, the Assessor will submit the completed assessment questionnaire, and the SPECTRIM workflow will route it to the level 1 reviewer. The Assessor is the only role allowed to make changes to an assessment questionnaire.

Reviewer

An optional role, the Reviewer is responsible for reviewing the accuracy of the assessment questionnaire and all related findings. This person should be knowledgeable of and have some responsibility over the subject matter area of the assessment component. The Reviewer will either accept or reject the assessment questionnaire. If the questionnaire is accepted, the SPECTRIM workflow will route the questionnaire to the Information Security Office. If the questionnaire is rejected, the SPECTRIM workflow will route the questionnaire back to the Assessor.

Information Security Office

The Information Security Office role refers to a team or a person at the organization. This team or designated person performs a quality assurance (QA) review of the assessment questionnaire responses. If the assessment questionnaire is rejected, it is returned to the Assessor. The Information Security Office or the designated person also works with the Assessor and others, as applicable, on the mitigation plan for the findings.

Organization Head

The Organization Head is responsible for approving the RAU if residual risk is high.

3.0 Risk Assessment Activity Summaries

For each risk assessment, the following activities must take place.

Activity 1: Create Risk Assessable Unit

Risk Assessment Coordinator Activity

The risk assessment process begins with the RAU. For the RAU, determine scope, frequency, and who the ISO designates as the final approver. In addition, an information owner can be designated. TAC 202 specifies, "Approval of the security risk acceptance, transference, or mitigation decision shall be the responsibility of the information security officer or his or her designee(s), in coordination with the information owner, for systems identified with a Low or Moderate residual risk."

Activity 2: Create Assessment Components

Risk Assessment Coordinator Activity

Within each RAU, assessment components are created. For each assessment component, the impact of the loss to the organization of the component being assessed must be determined.

Activity 3: Generate the Assessment Questionnaires

Risk Assessment Coordinator Activity

For each assessment component, an assessment questionnaire is generated. For each assessment questionnaire, determine and assign an Assessor, an optional Reviewer, and the Information Security Office designee.

Activity 4: Save the Risk Assessable Unit and Initiate Assessment Workflow

Risk Assessment Coordinator Activity

Create the RAUs, assessment components, and the assessment questionnaire for each assessment component.

Activity 5: Complete the Assessment Questionnaire

Assessor Activity

The Assessor receives an email requesting that he or she answer an assessment questionnaire.

Activity 6: Approve or Reject the Questionnaire

Reviewer Activity (If Assigned)

The reviewer receives an email requesting that he or she review and approve or reject an assessment questionnaire.

Activity 7: Approve or Reject the Questionnaire

Information Security Office Activity

The Information Security Office receives an email requesting that they review and approve or reject an assessment questionnaire.

Activity 8: Respond to Findings

Assessor Activity

The Assessor receives an email requesting that he or she respond to questionnaire findings. Click the link to log into SPECTRIM and choose to remediate findings or accept the risk.

Activity 9: Approve or Reject Finding Submission

Reviewer Activity (If Assigned)

The Reviewer receives an email requesting that he or she review and approve or reject the finding submission.

Activity 10: Forward Completed RAU to ISO for Approval

Risk Assessment Coordinator Activity

Coordinate responses to all questionnaires in the RAU. When all are complete, send to the ISO for approval.

Activity 11: Approve or Reject the RAU

Information Security Officer Activity

The ISO receives an email requesting that he or she review and approve or reject the RAU. Review and approve or reject the overall RAU in conjunction with the Business Owner. If residual risk is high, arrange to gain approval from the organization head.

Activity 12: Approve or Reject the RAU (if residual risk is high)

Organization Head Activity

If forwarded by the ISO, the person designated in the Organization Head field will receive an email to review and approve or reject the RAU.

4.0 Logging into SPECTRIM

1. Navigate to <https://dir.archerirm.us/>

The following login screen displays.



User Login

User Name:

Instance:

Password:

Login

> Display Domain

RSA Archer GRC
Powered by the RSA Archer GRC Platform™

2. Key in your User Name, Instance, and Password in the appropriate fields, and click **Login**.

Note: Your User Name is your email address, and your Instance is 20224. If you have not logged in within the past 60 days, your account will be deactivated. If you need to have your account reactivated or your password reset, email grc@dir.texas.gov.

5.0 Scoping the Assessment

Activity 1 – Create Risk Assessable Unit (RAU)

Risk Assessment Coordinator Activity

Note: You may see several tabs depending on which SPECTRIM components you have permission to access.

To create a new RAU:

1. Click the **Risk Management** tab.

*The **Risk Management Summary** screen displays.*

2. Click the **Risk Assessable Unit (Risk Project) – New Record** link in the lower right hand corner in the **Risk Quick Links** section.

The screenshot displays the 'Risk Management Summary' page. At the top, there is a header with the 'DIR' logo and 'Texas Department of Information Resources'. Below the header, there are tabs for 'Risk Management' and 'Support Request'. The main content area features a 'Risk Management Summary' section with a welcome message and a pie chart titled 'RAU by Overall Status'. The pie chart shows the following data:

| Status | Count | Percentage |
|---|-------|------------|
| Scoping | 2 | 40.00 % |
| Assessments and Findings Ready for Approval | 1 | 20.00 % |
| Sent Back for Revisions | 1 | 20.00 % |
| Approved | 1 | 20.00 % |

The right sidebar contains a 'For DIR GRC Support' section with the email 'grc@dir.texas.gov', a 'Confidentiality Statement' warning that information is confidential, and a 'Risk Quick Links' section. A red arrow points to the 'Risk Assessable Unit (Risk Project) - New Record' link in the quick links section.

The **Add New Record** screen displays.

Risk Assessable Unit (Risk Project): Add New Record

New Copy Save Apply View Delete Print

General Information

* Project Name: Overall Status:

* Organization: ... Frequency: Annual Biennial Special Purpose

Risk Project Description: Frequency Justification:

Risk Assessment Coordinator: Smith, Sally

Expected Start Date: Expected End Date:

Actual Start Date: 6/12/2015 Actual End Date:

Stakeholders

Information Owner: * ISO: ...

Organization Head: ...

3. Enter the data for your RAU.

Note: Red asterisks denote required fields.

General Information Section

- ***Project Name:** This is the name of your RAU. Consider creating a naming convention if you haven't already established one. Example: Organization Name: Information Security Program.
- ***Organization:** Select your organization from the list.
- ***Frequency:** Set the assessment frequency: annual, biennial, etc.
- **Risk Project Description:** Include a description of the item you are assessing.
- **Frequency Justification:** Select a reason for the frequency selection. If *Other* is selected, a text field will display, allowing you to further document the justification if necessary.
- **Risk Assessment Coordinator:** This field automatically populates with the name of the person creating the RAU.
- **Expected Start Date:** Choose the expected start date of your risk assessment using the date picker.
- **Expected End Date:** Choose the expected end date of your risk assessment using the date picker.
- **Actual Start Date:** This field automatically populates with today's date, but it can be changed.
- **Actual End Date:** This field automatically populates the date when the final approver accepts the RAU.

Stakeholders Section

▼ Stakeholders

Information Owner:

Organization Head:

* ISO:

- *Information Owner:* Since the ISO must approve risk assessments in conjunction with the Information Owner, enter the name of the Information Owner.
- **ISO:* Select the name of the ISO or the person designated to approve the RAU.
- *Organization Head:* Select the organization head if you want the RAU automatically routed in case of high residual risk. If the organization does not want the SPECTRIM workflow to directly email the Organization Head to initiate this approval, you can insert the RAC's name to delegate them to gain approval and document it according to organizational procedures.

4. Click **Apply** to save your work and continue updating.

Note: Clicking **Save** will save and exit from the screen.

Note: This is the second part of the new record screen for creating an RAU.

▼ Assessment Scoping

Please select the appropriate assessment components included in the scope of the assessment, including: applications, networks and locations. Once selected, please ensure that all components have appropriate security categories and NIST questionnaire types identified.

Once complete, please either select "Lookup" to see if there as has been a recent assessment for each component and if so, select the assessment to link it to the RAU; or, select "Add New" to add a new assessment for the related assessment component. (Note: when adding new assessments, the number of questions detailed in the questionnaire will be based on the NIST questionnaire type selected for each component.

As you add new assessments, please identify the Assessor, the Reviewer (if needed) and Security Office personell responsible for reviewing the assessment results. When ready you can then click launch assessments and the identified individuals will be notified that there is an assessment ready to be completed.

Recommended Security Category:

Applications

Locations

Networks

Organization Security Program Assessment

▼ Applications | Add New | Lookup |

| Information System Name | Organization Name | Application Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type |
|-------------------------|-------------------|-------------------|-------------------------------|-------------------|-------------------------|
| No Records Found | | | | | |

▼ Application Assessment(s) | Add New | Lookup |

| Questionnaire ID | Application | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
|------------------|-------------|-------------|----------|------------|---------------------------|---------------|---------------|
| No Records Found | | | | | | | |

Assessment Scoping Section

- *Recommended Security Category:* This field automatically populates with the highest security category of the risk assessment components that have been included in the RAU.

Note: Four tabs will display that correspond to the types of assessment components that comprise an RAU: Applications, Locations, Networks, and Organization Security Program Assessment.

Applications

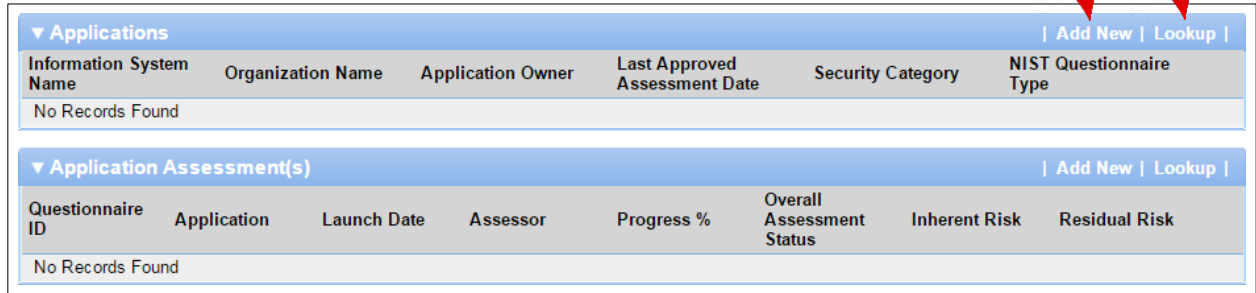
Locations

Networks

Organization Security Program Assessment

Applications and Application Assessment(s) Sections

Clicking on the Applications tab displays the following sections.



| ▼ Applications | | | | | | Add New Lookup |
|-------------------------|-------------------|-------------------|-------------------------------|-------------------|-------------------------|------------------|
| Information System Name | Organization Name | Application Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type | |
| No Records Found | | | | | | |

| ▼ Application Assessment(s) | | | | | | | Add New Lookup |
|-----------------------------|-------------|-------------|----------|------------|---------------------------|---------------|------------------|
| Questionnaire ID | Application | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
| No Records Found | | | | | | | |

- **Add New:** Use this option to add a new assessment component or a new questionnaire. See Activity 2: Create Risk Assessment Components on page 13 and Activity 3: Generate the Assessment Questionnaires on page 26.
- **Lookup:** Use this option to add a previously created assessment component or questionnaire.

5. Click **Apply** to save your work and keep updating.

Note: Clicking **Save** will save and exit from the screen.

Note: This is the third part of the new record screen for creating a risk assessable unit.

| ▼ Risk | | | |
|----------------------|--|----------------------|--|
| Inherent Risk: | <div style="width: 100%;"><div style="width: 100%;"></div></div> | Residual Risk: | <div style="width: 100%;"><div style="width: 100%;"></div></div> |
| Inherent Risk Score: | 92.11 | Residual Risk Score: | 94.74 |

| | | |
|-----------------------------|-----------------------------|----------------------------|
| Risk Assessment Coordinator | ISO/Business Owner Approval | Organization Head Approval |
|-----------------------------|-----------------------------|----------------------------|

| ▼ Risk Assessment Coordinator | |
|-------------------------------------|----------------------|
| Risk Assessment Coordinator Status: | Assessments Launched |
| Risk Coordinator Notes: | |

| ▼ Approval Document Attachments | | | |
|---------------------------------|------|------|-------------|
| Name | Size | Type | Upload Date |
| No Records Found | | | |

Risk Section

| ▼ Risk | | | |
|----------------------|--|----------------------|--|
| Inherent Risk: | <div style="width: 100%;"><div style="width: 100%;"></div></div> | Residual Risk: | <div style="width: 100%;"><div style="width: 100%;"></div></div> |
| Inherent Risk Score: | 92.11 | Residual Risk Score: | 94.74 |

- **Inherent Risk, Inherent Risk Score, Residual Risk, and Residual Risk Score:** This section will not display or contain scores until all associated assessment questionnaires have been submitted. No action is required.

Workflow Section

| | | |
|-------------------------------------|-----------------------------|----------------------------|
| Risk Assessment Coordinator | ISO/Business Owner Approval | Organization Head Approval |
| ▼ Risk Assessment Coordinator | | |
| Risk Assessment Coordinator Status: | Assessments Launched | |
| Risk Coordinator Notes: | | |

This section contains three tabs:

- Risk Assessment Coordinator – This tab is for the RAC to move the assessment through the process.
- ISO/Business Owner Approval – This tab is for the ISO to approve or reject the RAU or send it to the organization head if residual risk is high.
- Organization Head Approval – This tab is for the organization head to approve or reject the RAU.

Once the Assessment Questionnaires are launched, the Risk Assessment Coordinator should change the *Risk Assessment Coordinator Status* to *Assessments Launched*.

The other tabs are covered in section 10.0 Approving the Risk Assessable Unit on page 66.

Approval Document Attachments Section

| ▼ Approval Document Attachments | | | | |
|---------------------------------|------|------|-------------|--|
| Name | Size | Type | Upload Date | |
| No Records Found | | | | |

This section gives the RAC the ability to upload meeting minutes, emails, etc., to document the organization head's acceptance of the RAU.

6. Click **Apply** to save your work and keep updating.

Note: Clicking **Save** will save and exit from the screen.

Activity 2: Create Risk Assessment Components

Risk Assessment Coordinator Activity

Activity 2a: Create an Application Risk Assessment Component

When the RAC determines the scope of the assessment, they must add the components and questionnaires.

1. If an application must be assessed, click the **Applications** tab.

| Information System Name | Organization Name | Application Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type |
|-------------------------|-------------------|-------------------|-------------------------------|-------------------|-------------------------|
| No Records Found | | | | | |

| Questionnaire ID | Application | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
|------------------|-------------|-------------|----------|------------|---------------------------|---------------|---------------|
| No Records Found | | | | | | | |

– OR –

If the application is already stored in SPECTRIM, click **Lookup** in the **Applications** section.

The following screen displays.

| <input type="checkbox"/> | Information System Name | Organization Name | Application Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type |
|--------------------------|--------------------------------|-------------------------|--------------------------------|-------------------------------|-------------------|-------------------------|
| <input type="checkbox"/> | Employee Payroll System | State Agency for Archer | Sally_Smith | | Low | |
| <input type="checkbox"/> | Employee Leave System | State Agency for Archer | Osbourne_Sam | | Low | |
| <input type="checkbox"/> | Employee Leave Tracking System | State Agency for Archer | Collins_Rachel | 5/5/2015 | Low | NIST Low |

2. Select the check box next to the application you want to include. Then click **OK** to return to the RAU screen.
3. Click **Apply** to save your work and keep updating.

Note: Clicking **Save** will save and exit from the screen.

- If the application is not stored in SPECTRIM, click **Add New**.

This is the first part of the **Applications: Add New Record** screen that displays.

The screenshot shows a web application window titled "Applications: Add New Record". The window has a blue header bar with the title and standard window controls (minimize, maximize, close). Below the header is a toolbar with icons for "New", "Copy", "Save", "Apply", "View", "Delete", "Print", and "Email". The main content area is divided into sections. At the top is a grey bar with a right-pointing arrow and the text "About". Below that is a blue bar with a downward-pointing arrow and the text "General Information". Under "General Information", there are several fields: "Information System Name" (with a red asterisk), "Application Owner", "Location(s)", "Network(s)", "Organization", "Status" (a dropdown menu currently showing "Active"), "Regulatory Drivers", and "Security Category". There is also a large text area for "Application Description".

Note: Red asterisks denote required fields.

General Information Section

- **Information System Name:* Enter the name of the information system to be assessed.
- *Organization:* Choose the name of the organization associated with the *Information System Name*.
- *Application Owner:* Choose an application owner if the Application Owner has an account in SPECTRIM. If the application owner does not have an account in SPECTRIM, leave it blank.
- *Status:* Indicate whether an application is Active or Inactive.
- *Location(s):* Link an application to a location such as datacenter, server room, etc., if the location has been previously saved in SPECTRIM. If you enter a location later, you can link the two together later.
- *Regulatory Drivers:* Choose which regulations apply to this application.
- *Network(s):* Link an application to a network if the network has been previously saved in SPECTRIM. If you enter a network later, you can link the two together later.
- *Application Description:* Enter a description of the application.

- Click **Apply** to save your work and keep updating.

Note: Clicking **Save** will save and exit from the screen.

This is the second part of the **Applications: Add New Record** screen that displays.

Information Types Section

| Information Types | | | | | | | Lookup |
|-------------------|------------------------|--|------------------|----------------------------------|---------------------|-------------------------------------|--------|
| Information Type | Confidentiality Rating | Confidentiality Special Considerations | Integrity Rating | Integrity Special Considerations | Availability Rating | Availability Special Considerations | |
| No Records Found | | | | | | | |

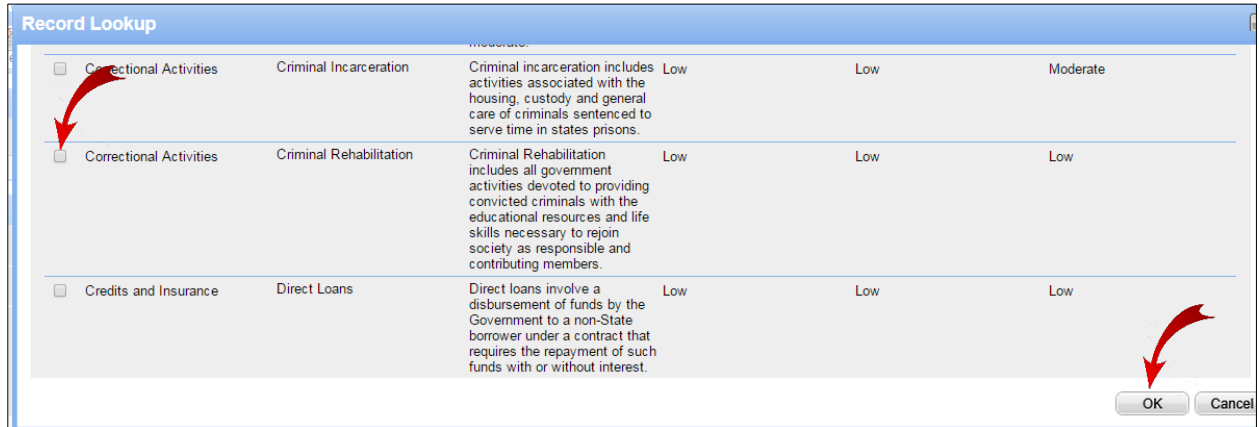
Information type comes from [NIST SP 800-60 Volume 2 "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories"](#), which describes a standard way to determine the level of NIST controls you will be assessing the application against.

- Click **Lookup**.

The following screen displays.

| Information Type | Confidentiality Rating | Confidentiality Special Considerations | Integrity Rating | Integrity Special Considerations | Availability Rating | Availability Special Considerations |
|--|-------------------------|---|------------------|----------------------------------|---------------------|-------------------------------------|
| <input type="checkbox"/> Correctional Activities | Criminal Incarceration | Criminal incarceration includes activities associated with the housing, custody and general care of criminals sentenced to serve time in states prisons. | Low | | Low | Moderate |
| <input type="checkbox"/> Correctional Activities | Criminal Rehabilitation | Criminal Rehabilitation includes all government activities devoted to providing convicted criminals with the educational resources and life skills necessary to rejoin society as responsible and contributing members. | Low | | Low | Low |
| <input type="checkbox"/> Credits and Insurance | Direct Loans | Direct loans involve a disbursement of funds by the Government to a non-State borrower under a contract that requires the repayment of such funds with or without interest. | Low | | Low | Low |

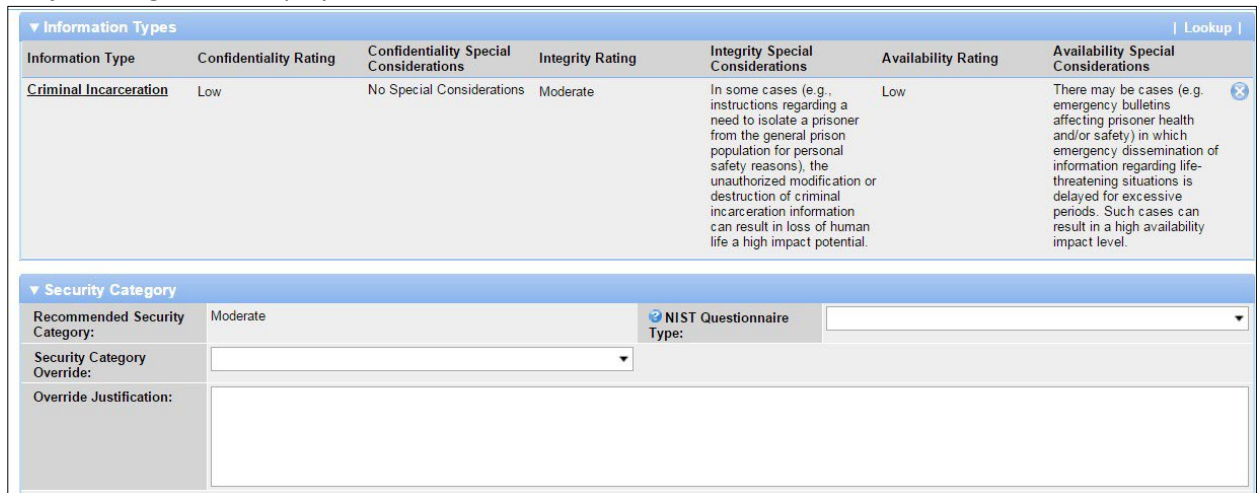
- Click the checkbox next to the information type corresponding to your application, and then click **OK**.



The Application Screen is now populated with the information type you selected, the confidentiality, integrity, and availability ratings, and any special considerations about that information type.

- Click **Apply** to populate the recommended Security Category with the high level of the Confidentiality, Integrity, and Availability ratings.

The following screen displays the results.



Security Category Section

As shown in the example screen, there are special considerations for Integrity and Availability in the example Information Types selected.

Application Assessment(s): 209121

0 of 43 Completed | Options

This questionnaire is in a Development status. It is not licensed for Production.

History Log.

▼ Comments

| Question Name | Submitter | Date | Comment | Attachment |
|------------------|-----------|------|---------|------------|
| No Records Found | | | | |

▼ Access Control

| | | |
|--|--|--------------------------|
| <input checked="" type="checkbox"/> NIST-R0002-AC-02: | Are there processes in place to ensure access provided to users (e.g., the role provided to a user for an application, or privileged access provided to an IT administrator, etc.) aligns with business requirements and/or access control policy? [Note: an example could be documented approval from asset/business owner, timely removal of access from transferred or terminated employees, etc.] | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> NIST-R0003-AC-03.02: | Are information systems (Application Assessments; operating systems; Network Assessment devices; databases; etc.) configured and access enforcement mechanisms employed per approved policy to provide protection from unauthorized access by malicious users; software or systems? | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> NIST-R0007-AC-07: | Have you implemented procedures and controls to lock user access to information resources after a defined number of unsuccessful login attempts? | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> NIST-R0008-AC-08: | Do organizational or departmental information systems display an approved system use notification message or banner before granting access to the information system? | <input type="checkbox"/> |

Edit Cancel

Note: Red asterisks denote required fields.

- **Security Category Override:** Change the *Recommended Security Category* based on these special considerations.
- ***Override Justification:** You will be required to enter a justification if you choose to override the *Recommended Security Category*.
- **NIST Questionnaire Type:** Select the corresponding NIST Questionnaire Type. This is the questionnaire that will be answered to assess risk for this application. There are six choices for this field: NIST Low, NIST Moderate, and NIST High have questions for each NIST 800-53 control while NIST Detailed Low, NIST Detailed Moderate, and NIST Detailed High have questions for every line of every control in NIST 800-53. The following table shows the number of questions for each questionnaire type and each NIST control level.

Note: If you do not select a NIST Questionnaire type, it will default to NIST Low.

| | | | | |
|-------------|------------------------|-----|---------------|-----|
| Sec Program | NIST Detailed Low | 296 | NIST Low | 104 |
| | NIST Detailed Moderate | 392 | NIST Moderate | 131 |
| | NIST Detailed High | 423 | NIST High | 162 |
| Location | NIST Detailed Low | 101 | NIST Low | 35 |
| | NIST Detailed Moderate | 171 | NIST Moderate | 51 |
| | NIST Detailed High | 221 | NIST High | 101 |
| Network | NIST Detailed Low | 137 | NIST Low | 38 |
| | NIST Detailed Moderate | 220 | NIST Moderate | 57 |
| | NIST Detailed High | 270 | NIST High | 107 |
| Application | NIST Detailed Low | 148 | NIST Low | 43 |
| | NIST Detailed Moderate | 220 | NIST Moderate | 61 |
| | NIST Detailed High | 260 | NIST High | 101 |

Table 1– Number of Questions per Assessment Questionnaire Type

This is the third part of the **Applications: Add New Record** that displays.

| | | | | | | | | |
|---|----------|---------------|------------|---------------------------|---------------------|---------------|---------------------|---------------|
| Additional Documentation Add New | | | | | | | | |
| Name | | Size | | | | | | |
| No Records Found | | | | | | | | |
| ▼ Application Security Assessment(s) | | | | | | | | |
| Last Approved Assessment Date: | | | | | | | | |
| Inherent Risk Score: | | | | Residual Risk Score: | | | | |
| Application Assessment(s) Add New | | | | | | | | |
| Questionnaire ID | Assessor | Launch Date ▼ | Progress % | Overall Assessment Status | Inherent Risk Score | Inherent Risk | Residual Risk Score | Residual Risk |
| No Records Found | | | | | | | | |
| ▶ History Log | | | | | | | | |

Additional Documentation Section

| | | | | | | | | |
|---|--|------|--|--|--|--|--|--|
| Additional Documentation Add New | | | | | | | | |
| Name | | Size | | | | | | |
| No Records Found | | | | | | | | |



Click **Add New** to upload additional documentation.

Application Security Assessment(s) Section

| | | | | | | | | |
|--------------------------------------|----------|---------------|------------|---------------------------|---------------------|---------------|---------------------|---------------|
| ▼ Application Security Assessment(s) | | | | | | | | |
| Last Approved Assessment Date: | | | | | | | | |
| Inherent Risk Score: | | | | Residual Risk Score: | | | | |
| Application Assessment(s) Add New | | | | | | | | |
| Questionnaire ID | Assessor | Launch Date ▼ | Progress % | Overall Assessment Status | Inherent Risk Score | Inherent Risk | Residual Risk Score | Residual Risk |
| No Records Found | | | | | | | | |

This section shows previous Application Security Assessment data, including the date and scores of the last assessment and links to previous questionnaires.

History Log Section

| | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|
| ▶ History Log | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|

This section displays a History Log showing actions taken on this record.

9. Click **Save** to return to the RAU screen.

Activity 2b: Create a Location Risk Assessment Component Risk Assessment Coordinator Activity

Location Information Section

Once the RAC determines the scope of the assessment, they will need to add the components and questionnaires. If you need to include a location in the assessment, click the **Locations** tab.

1. If the location is already stored in SPECTRIM, click **Lookup** in the **Location Information** section.

| Location Information | | | | | | Add New Lookup |
|----------------------|-------------------|----------------|-------------------------------|-------------------|-------------------------|--|
| Location Name | Organization Name | Location Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type | |
| No Records Found | | | | | | |

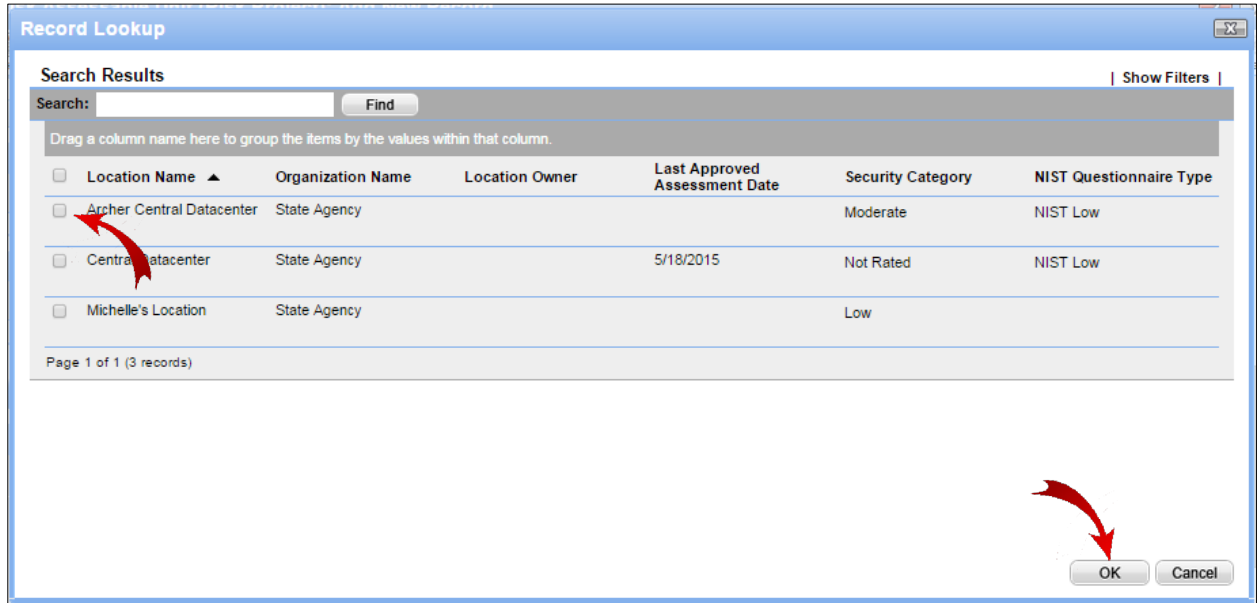
| Location Assessment(s) | | | | | | | | Add New Lookup |
|------------------------|----------|-------------|----------|------------|---------------------------|---------------|---------------|--|
| Questionnaire ID | Location | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk | |
| No Records Found | | | | | | | | |

The following screen displays.

| Search Results | | | | | | Show Filters |
|--|---------------------------|----------------|-------------------------------|-------------------|-------------------------|------------------------------|
| Search: <input type="text"/> <input type="button" value="Find"/> | | | | | | |
| Drag a column name here to group the items by the values within that column. | | | | | | |
| <input type="checkbox"/> Location Name ▲ | Organization Name | Location Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type | |
| <input type="checkbox"/> | Archer Central Datacenter | State Agency | | Moderate | NIST Low | |
| <input type="checkbox"/> | Central Datacenter | State Agency | 5/18/2015 | Not Rated | NIST Low | |
| <input type="checkbox"/> | Michelle's Location | State Agency | | Low | | |

Page 1 of 1 (3 records)

2. Select the checkbox next to the location you want to include, and then click **OK** to return to the RAU screen.

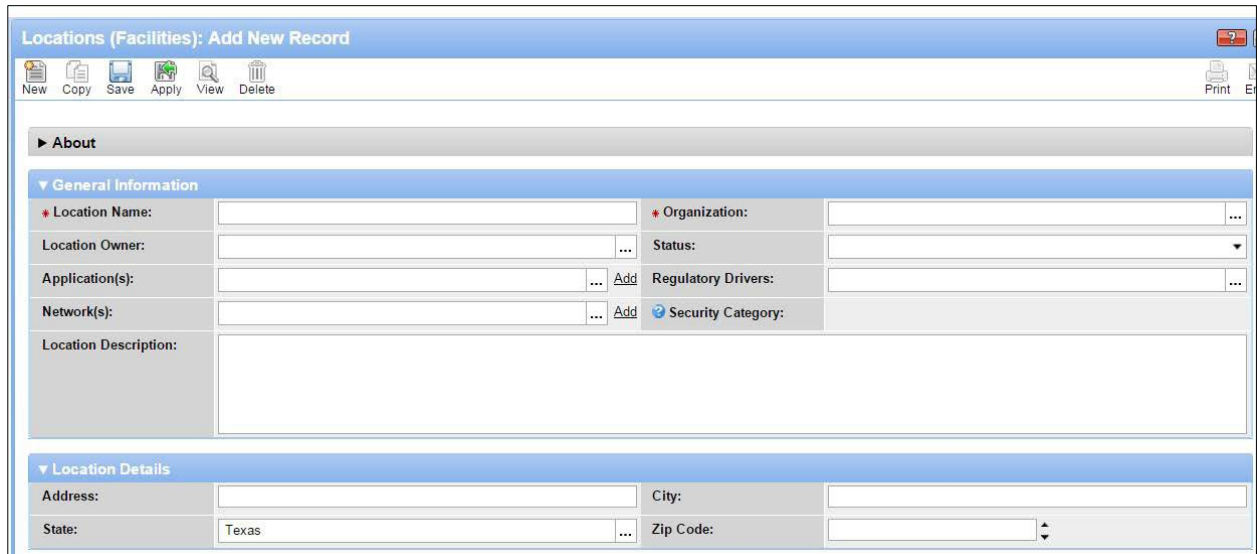


3. Click **Apply** to save your work and continue updating.

Note: Clicking **Save** will save and exit from the screen.

4. If the location is not stored in SPECTRIM, click **Add New**.

*This is the first part of the **Locations (Facilities): Add New Record** section that will display.*



General Information Section

Note: Red asterisks denote required fields.

- **Location Name:* Enter the name of the location/facility to be assessed.
- **Organization:* Populate this field with the organization that it is associated to.
- *Location Owner:* If the location owner has an account in SPECTRIM, click the ellipses to select one from the list.
- *Status:* Indicate whether a location is active or inactive.
- *Application(s):* Link a location to an application if the application has been previously saved in SPECTRIM.
- *Regulatory Drivers:* Select which regulations apply to this location.
- *Network:* Link a location to a network if the network has been previously saved in SPECTRIM.
- *Location Description:* Key in a description of the location.

Location Details Section

- *Address:* The physical address of the location.
- *City*
- *State*
- *Zip Code*

This is the second part of the **Locations (Facilities): Add New Record** section that will display.

| ▼ Security Category | | | | | | | | | |
|---|----------|-------------|------------|---------------------------|---------------|---------------------|---------------|---------------------|--|
| Recommended Security Category: | | | | NIST Questionnaire Type: | | | | | |
| Additional Documentation Add New | | | | | | | | | |
| Name | | Size | | | | | | | |
| No Records Found | | | | | | | | | |
| ▼ Location Assessment(s) | | | | | | | | | |
| Last Approved Assessment Date: | | | | | | | | | |
| Inherent Risk Score: | | | | Residual Risk Score: | | | | | |
| Location Assessment(s) | | | | | | | | | |
| Questionnaire ID | Assessor | Launch Date | Progress % | Overall Assessment Status | Inherent Risk | Inherent Risk Score | Residual Risk | Residual Risk Score | |
| No Records Found | | | | | | | | | |
| ▶ History Log | | | | | | | | | |







Security Category Section

- *Recommended Security Category:* The security category value comes from the Application. If you do not have an application associated above, this will display as *Not Rated* once you save the record. If you wish to have a security category populate, add the appropriate application.
- *NIST Questionnaire Type:* Select the corresponding NIST Questionnaire Type. This is the questionnaire that will be answered to assess risk for this location. There are six choices for this field: NIST Low, NIST Moderate, and NIST High (these have questions for each NIST 800-53 control) NIST Detailed Low, NIST Detailed Moderate, and NIST Detailed High (these have questions for every line of every control in NIST 800-53). Table 1 shows the number of questions for each questionnaire type and each NIST control level.


Note: If you do not select a NIST Questionnaire type, it will default to NIST Low.

- *Additional Documentation*: Click **Add New** to upload additional, pertinent documentation.
- *Location Assessment(s)*: Shows past Location Assessment data, including the date and risk scores of the last assessment, and links to the past questionnaires.
- *History Log*: Shows all actions taken on this record.
-

Risk Assessable Unit (Risk Project): Add New Record

▼ General Information

 * **Project Name:**

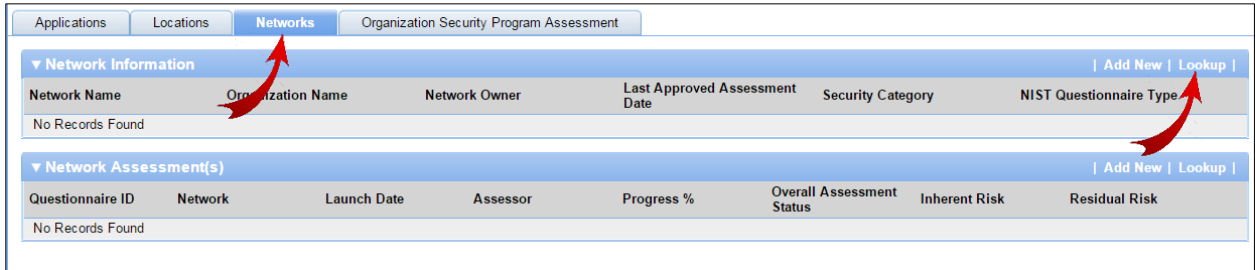
5. Click **Save** to return to the RAU screen.
6. Click **Apply** to save your work and continue updating.

Note: Clicking **Save** will save and exit from the screen.

Activity 2c: Create a Network Risk Assessment Component
Risk Assessment Coordinator Activity

Network Information Section

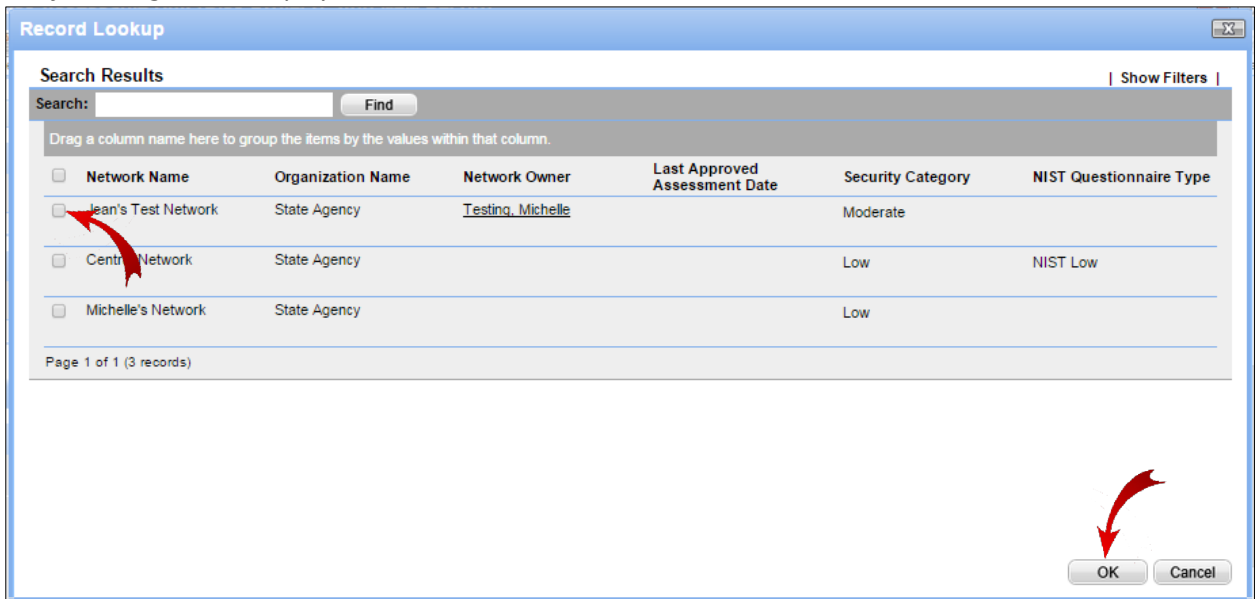
1. Once the RAC determines the scope of the assessment, they must add the components and questionnaires. If a network must be assessed or an assessment must be added to, click the **Networks** tab.



– OR –

If the network is already stored in SPECTRIM, click **Lookup**.

The following screen displays.



2. Click the checkbox next to the network you want to include, and then click **OK** to return to the RAU screen.

Risk Assessable Unit (Risk Project): Add New Record



▼ General Information

Project Name:

3. Click **Apply** to save your work and continue updating.

Note: Clicking **Save** will save and exit from the screen.

4. If the network is not stored in SPECTRIM, click **Add New**.

This is the first part of the **Networks: Add New Record** that will display.

A screenshot of a web application window titled "Networks: Add New Record". The window has a blue header bar with the title and a help icon. Below the header is a toolbar with icons for New, Copy, Save, Apply, View, and Delete, and a Print icon on the right. A red banner below the toolbar contains the text: "This application is in a Development status. It is not licensed for Production." The main content area is a form titled "General Information". The form has several fields: "* Network Name:" (required), "Network Owner:", "Application(s):" (with an "Add" link), "Location(s):" (with an "Add" link), "Network Description:" (a large text area), "* Organization:" (required), "Status:" (a dropdown menu), "Regulatory Drivers:" (with an "Add" link), and "Security Category:". The "Add" links are blue and have a plus sign.

Note: Red asterisks denote required fields.

General Information Section

***Network Name:** Key in the name of the information system to be assessed.

***Organization:** Populate this field with the organization that it is associated to.

Network Owner: You can select a network owner from the list appearing (if the network owner has an account in SPECTRIM).

Status: You can show that a network is active or inactive.

Application(s): You can link a network to an application if the application has been previously saved in SPECTRIM.

Regulatory Drivers: You can select what regulations apply to this network in this field.

Location(s): You can link a network to a location if the location has been previously saved in SPECTRIM.

Network Description: Consider entering a description of the network.

This is the second part of the **Networks: Add New Record** that will display.

| Questionnaire ID | Network | Assessor | Progress % | Overall Assessment Status | Launch Date | Inherent Risk | Inherent Score | Residual Risk | Residual Score |
|------------------|---------|----------|------------|---------------------------|-------------|---------------|----------------|---------------|----------------|
| No Records Found | | | | | | | | | |

Security Category Section

- *Recommended Security Category:* The security category value comes from the Application. If you do not have an application associated above, this will display as “Not Rated” once you save the record. If you wish to have a security category populate, make sure to add the appropriate application.
- *NIST Questionnaire Type:* Select the corresponding NIST Questionnaire Type from the drop down box. This will be the questionnaire that will be answered to assess risk for this network. There are six different selections for this field. NIST Low, NIST Moderate and NIST High have questions for each NIST 800-53 control while NIST Detailed Low, NIST Detailed Moderate, and NIST Detailed High have questions for every line of every control in NIST 800-53. Table 1 shows the number of questions for each questionnaire type and each NIST control level.

Note: If you do not select a NIST Questionnaire type, it will default to NIST Low.

Risk Assessable Unit (Risk Project): Add New Record



Project Name:

5. Click **Save** to return to the RAU screen.

– OR –

Click **Apply** to save your work and keep updating.

Note: Clicking **Save** will save and exit from the screen.

Activity 3: Generate the Assessment Questionnaires

Activity 3a: Create an Application Assessment

Risk Assessment Coordinator Activity

Application Assessment(s) Section

Once the application has been associated to the RAU, you can add the assessment questionnaire.

1. To associate an existing questionnaire to the RAU, click **Lookup** in the **Application Assessment(s)** section.

| Information System Name | Organization Name | Application Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type |
|-------------------------|-------------------|-------------------|-------------------------------|-------------------|-------------------------|
| No Records Found | | | | | |

| Questionnaire ID | Application | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
|------------------|-------------|-------------|----------|------------|---------------------------|---------------|---------------|
| No Records Found | | | | | | | |

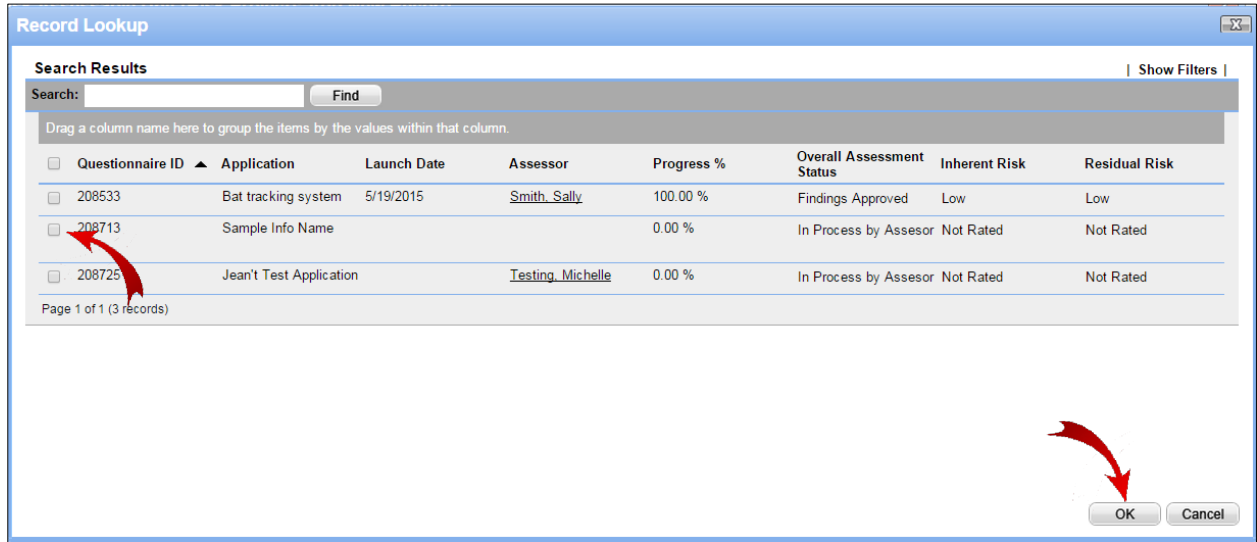
The following screen displays.

| Questionnaire ID | Application | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
|---------------------------------|-------------------------|-------------|--------------------------|------------|---------------------------|---------------|---------------|
| <input type="checkbox"/> 208533 | Bat tracking system | 5/19/2015 | <u>Smith, Sally</u> | 100.00 % | Findings Approved | Low | Low |
| <input type="checkbox"/> 208713 | Sample Info Name | | | 0.00 % | In Process by Assesor | Not Rated | Not Rated |
| <input type="checkbox"/> 208725 | Jean't Test Application | | <u>Testing, Michelle</u> | 0.00 % | In Process by Assesor | Not Rated | Not Rated |

Page 1 of 1 (3 records)

OK Cancel

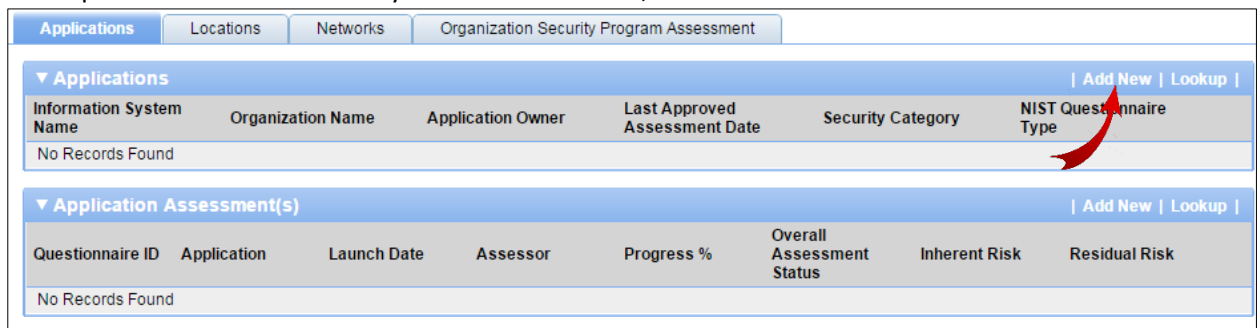
2. Select the checkbox next to the questionnaire you want to include, and then click **OK** to return to the RAU screen.



3. Click **Apply** to save your work and continue updating.

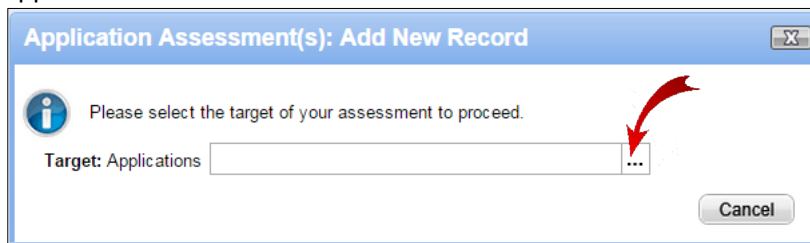
Note: Clicking **Save** will save and exit from the screen.

4. If the questionnaire is not already stored in SPECTRIM, click **Add New**.



*The **Application Assessment(s): Add New Record** screen displays.*

5. Associate your application to the questionnaire. Click the ellipses and select the appropriate application.



6. Click **Apply**.

The *Application Assessment(s)* screen displays.

Application Assessment(s): 209087

0 of 43 Completed | Options ▾

This questionnaire is in a Development status. It is not licensed for Production.

► Instructions

General Information

| | | | |
|------------------------------|--|----------------------------|--------------------------|
| Questionnaire ID: | 209087 | Overall Assessment Status: | In Process by Assesor |
| * Application: | Bat tracking system | Progress %: | 0.00 % |
| Organization Name: | State Agency | Due Date: | <input type="text"/> |
| Risk Assessment Coordinator: | | * Assessor: | <input type="text"/> ... |
| Launch Assessment: | <input type="radio"/> Yes <input type="radio"/> No | Reviewer: | <input type="text"/> ... |
| Launch Date: | <input type="text"/> | * Security Office: | <input type="text"/> ... |
| History Log: | View History Log | | |

▼ Comments

| Question Name | Submitter | Date | Comment | Attachment |
|------------------|-----------|------|---------|------------|
| No Records Found | | | | |

General Information Section

Note: Red asterisks denote required fields.

- *Questionnaire ID:* Automatically generated by SPECTRIM.
- *Overall Status:* Automatically populated by SPECTRIM, as is **Organization Name*, **Application*, and *Progress*.

Note: The *Risk Assessment Coordinator* field is blank. Once you save this questionnaire and then save the RAU, the field will be populated. It is important to make sure this happens so you know that the questionnaire is linked to the RAU.

- *Due Date:* Enter the date the assessment questionnaire is due.
- **Assessor:* Select an assessor to answer the questions.
- *Reviewer:* Select a reviewer to review the answers (optional).
- **Security Office:* Select a member of your Security Office to review the assessment.
- *Launch Assessment:* Do not launch the assessment until the RAU has been saved.
- *Launch Date:* SPECTRIM will automatically populate this field.
- *History Log:* Shows a log of all actions taken on this questionnaire.

Comments Section

- *Comments:* This will display all comments attached to a question on the assessment as it is being processed.

7. Click **Save and Close** to return to the RAU record.

Risk Assessable Unit (Risk Project): Add New Record



▼ General Information

* Project Name:

- Click **Apply** to save your work and continue updating.

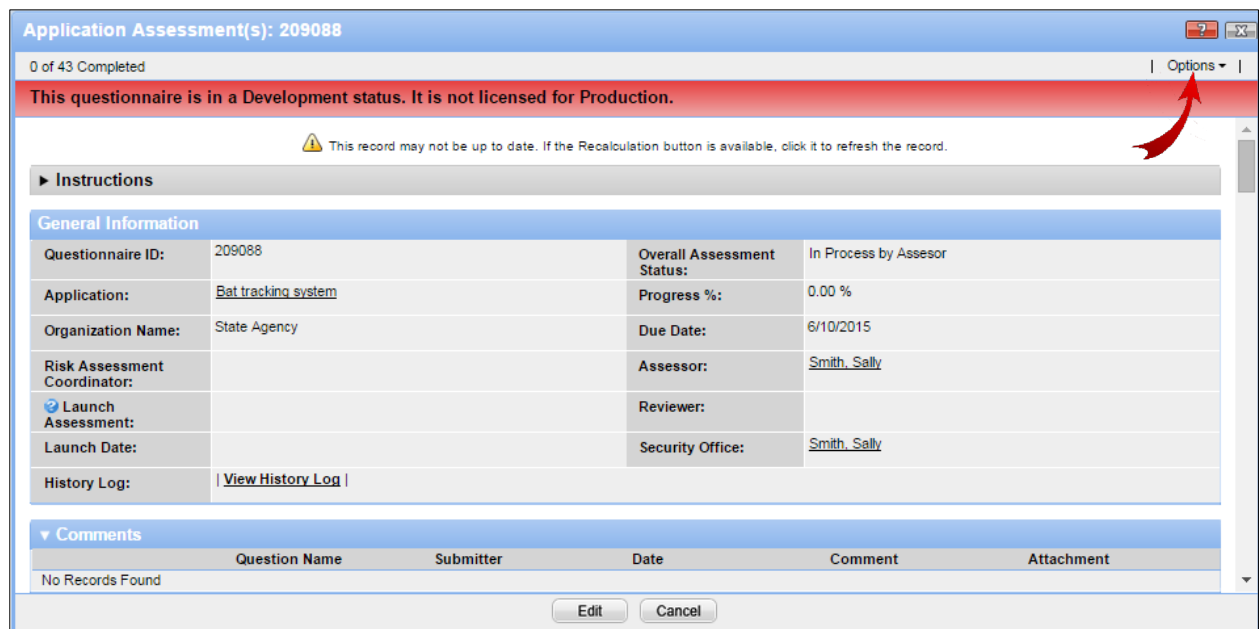
Note: Clicking **Save** will save and exit from the screen.

- When you next open the assessment questionnaire, you may see the following text at the top of the screen:

"This record may not be up to date. If the Recalculation button is available, click it to refresh the record."

Click the **Options** dropdown to expose the **Recalculation** option and select it.

Note: The **Risk Assessment Coordinator** field is blank.



Application Assessment(s): 209088

0 of 43 Completed

This questionnaire is in a Development status. It is not licensed for Production.

⚠ This record may not be up to date. If the Recalculation button is available, click it to refresh the record.

► Instructions

General Information

| | | | |
|------------------------------|-------------------------------------|----------------------------|------------------------------|
| Questionnaire ID: | 209088 | Overall Assessment Status: | In Process by Assesor |
| Application: | Bat tracking system | Progress %: | 0.00 % |
| Organization Name: | State Agency | Due Date: | 6/10/2015 |
| Risk Assessment Coordinator: | | Assessor: | Smith, Sally |
| Launch Assessment: | | Reviewer: | |
| Launch Date: | | Security Office: | Smith, Sally |
| History Log: | View History Log | | |

▼ Comments

| Question Name | Submitter | Date | Comment | Attachment |
|------------------|-----------|------|---------|------------|
| No Records Found | | | | |

Edit Cancel

After clicking **Recalculation**, the name of the Risk Assessment Coordinator displays.

- Choose the **Yes** radio button next to **Launch Assessment** to launch the assessment, and then click **Save and Close**.

Application Assessment(s): 209088

0 of 43 Completed | Options

This questionnaire is in a Development status. It is not licensed for Production.

► Instructions

General Information

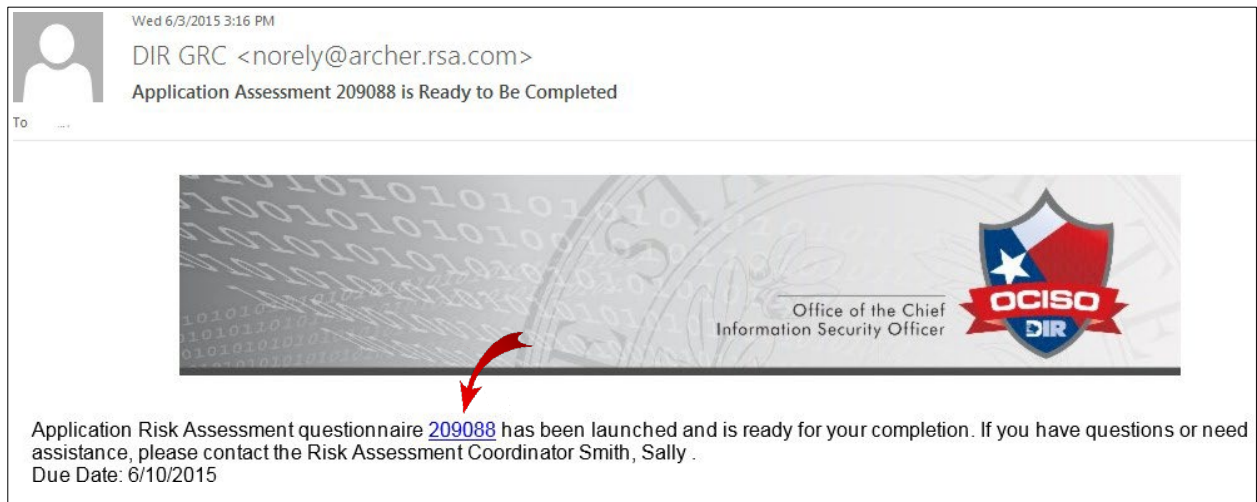
| | | | |
|------------------------------|---|----------------------------|-----------------------|
| Questionnaire ID: | 209088 | Overall Assessment Status: | In Process by Assesor |
| * Application: | Bat training system | Progress %: | 0.00 % |
| Organization Name: | State Agency | Due Date: | 6/10/2015 |
| Risk Assessment Coordinator: | Smith, Sally | * Assessor: | Smith, Sally |
| Launch Assessment: | <input checked="" type="radio"/> Yes <input type="radio"/> No | Reviewer: | |
| Launch Date: | 6/3/2015 | * Security Office: | Smith, Sally |
| History Log: | View History Log | | |

▼ Comments

| Question Name | Submitter | Date | Comment | Attachment |
|------------------|-----------|------|---------|------------|
| No Records Found | | | | |

Save and Close Save and Continue Cancel

The Assessor will receive an email with a link to the questionnaire indicating that they must complete an assessment. Selecting the link requires them to authenticate. The questionnaire will open.



Activity 3b: Create a Location Assessment
Risk Assessment Coordinator Activity

Location Assessment(s) Section

Once the location has been associated to the RAU, you can add the Assessment Questionnaire.

1. To associate an existing questionnaire to the RAU, click **Lookup** in the **Location Assessment(s)** section.

The screenshot shows a web application interface with tabs for 'Applications', 'Locations', 'Networks', and 'Organization Security Program Assessment'. The 'Locations' tab is active. Below the tabs are two sections:

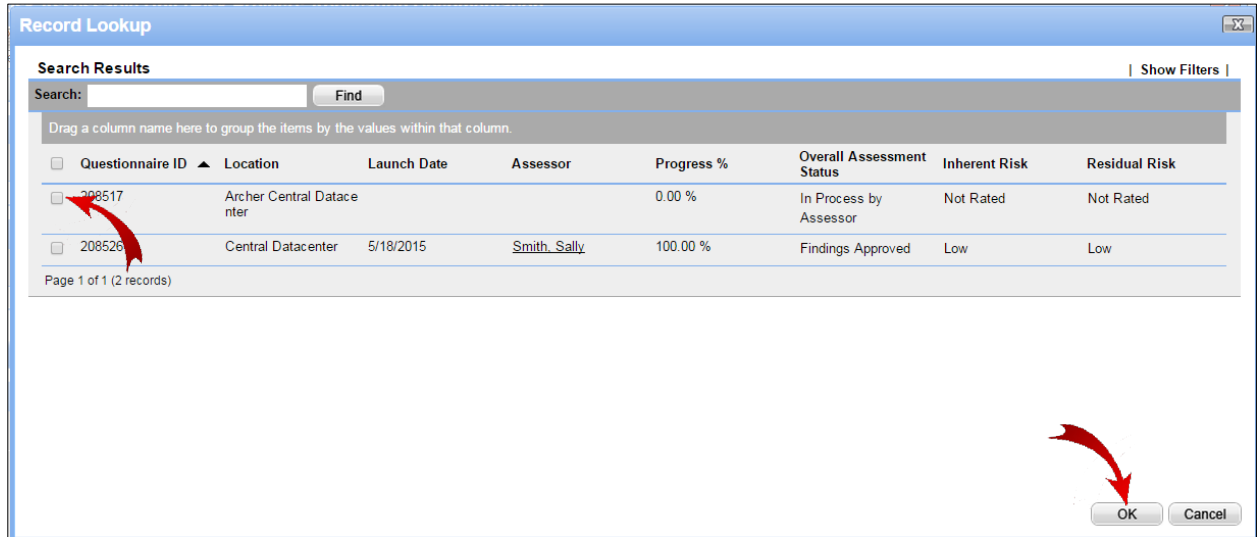
- Location Information**: A table with columns: Location Name, Organization Name, Location Owner, Last Approved Assessment Date, Security Category, and NIST Questionnaire Type. Below the table, it says 'No Records Found'. A red arrow points to the 'Lookup' link in the top right corner of this section.
- Location Assessment(s)**: A table with columns: Questionnaire ID, Location, Launch Date, Assessor, Progress %, Overall Assessment Status, Inherent Risk, and Residual Risk. Below the table, it says 'No Records Found'.

The following screen displays.

The 'Record Lookup' dialog box displays search results for assessment questionnaires. It includes a search bar, a 'Find' button, and a table of results. Below the table, it indicates 'Page 1 of 1 (2 records)'. At the bottom right, there are 'OK' and 'Cancel' buttons.

| Questionnaire ID | Location | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
|---------------------------------|---------------------------|-------------|------------------------------|------------|---------------------------|---------------|---------------|
| <input type="checkbox"/> 208517 | Archer Central Datacenter | | | 0.00 % | In Process by Assessor | Not Rated | Not Rated |
| <input type="checkbox"/> 208526 | Central Datacenter | 5/18/2015 | Smith, Sally | 100.00 % | Findings Approved | Low | Low |

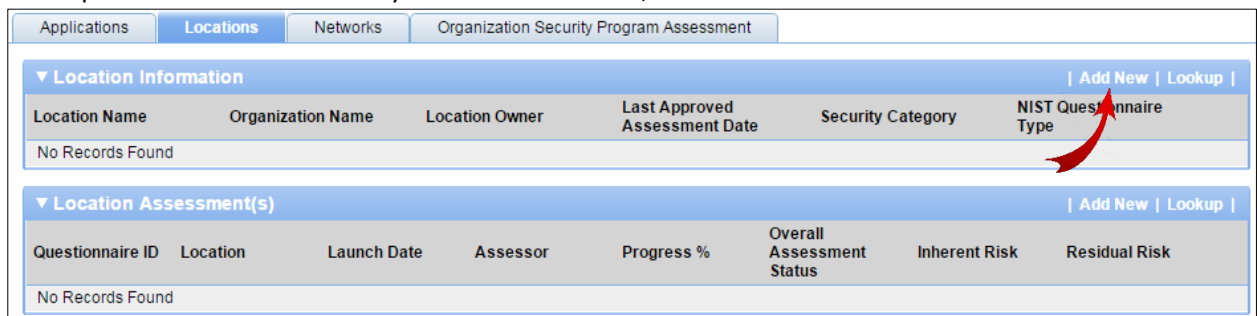
2. Select the checkbox next to the questionnaire you want to include, and then click **OK** to return to the RAU screen.



3. Click **Apply** to save your work and continue updating.

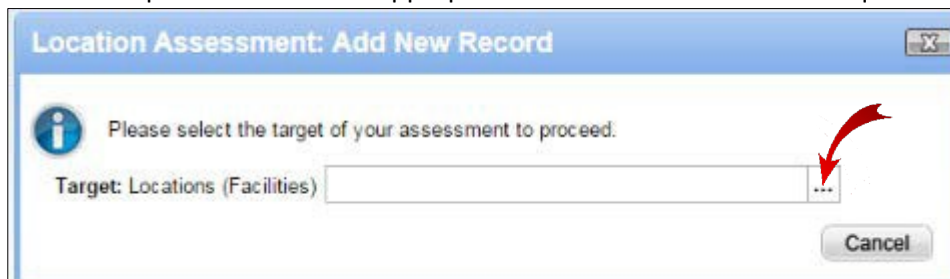
Note: Clicking **Save** will save and exit from the screen.

4. If the questionnaire is not already stored in SPECTRIM, click **Add New**.



*The **Location Assessment: Add New Record** screen displays.*

5. Click the ellipses and select the appropriate location to associate to the questionnaire.



6. Click **Apply**.

The *Location Assessment(s)* screen displays.

| General Information | | | |
|------------------------------|--|----------------------------|------------------------|
| Questionnaire ID: | 209089 | Overall Assessment Status: | In Process by Assessor |
| * Location: | Archer Central Datacenter | Progress %: | 0.00 % |
| Organization Name: | State Agency | Due Date: | <input type="text"/> |
| Risk Assessment Coordinator: | | * Assessor: | <input type="text"/> |
| Launch Assessment: | <input type="radio"/> Yes <input type="radio"/> No | Reviewer: | <input type="text"/> |
| Launch Date: | <input type="text"/> | * Security Office: | <input type="text"/> |
| History Log: | View History Log | | |

General Information Section

Note: Red asterisks denote required fields.

- *Questionnaire ID:* Automatically generated by SPECTRIM.
- *Overall Status:* Automatically populated by SPECTRIM, as is **Organization Name*, **Location*, and *Progress*.

Note: The *Risk Assessment Coordinator* field is blank. Once you save this questionnaire and then save the RAU, the field will be populated. It is important to make sure this happens so you know that the questionnaire is linked to the RAU.

- *Due Date:* Enter the date the assessment questionnaire is due.
- **Assessor:* Select an assessor to answer the questions.
- *Reviewer:* Select a reviewer to review the answers (optional).
- **Security Office:* Select a member of the Security Office to review the assessment.
- *Launch Assessment:* Do not launch the assessment until the RAU has been saved.
- *Launch Date:* SPECTRIM will automatically populate this field.
- *History Log:* Shows a log of all actions taken on this questionnaire.

Comments Section

- *Comments:* Displays all comments attached to a question on the assessment as it is being processed.

7. Click **Save and Close** to return to the RAU record.

8. Click **Apply** to save your work and continue updating.

Note: Clicking **Save** will save and exit from the screen.

9. When you next open the assessment questionnaire, you may see the following text at the top of the screen:

“This record may not be up to date. If the Recalculation button is available, click it to refresh the record.”

Click the **Options** dropdown to expose the **Recalculation** option and select it.

Note: The **Organization Name** and **Risk Assessment Coordinator** fields are blank.

| General Information | | | |
|------------------------------|---|----------------------------|------------------------------|
| Questionnaire ID: | 209089 | Overall Assessment Status: | In Process by Assessor |
| Location: | Archer Central Datacenter | Progress %: | 0.00 % |
| Organization Name: | State Agency | Due Date: | 6/10/2015 |
| Risk Assessment Coordinator: | Smith, Sally | Assessor: | Smith, Sally |
| Launch Assessment: | | Reviewer: | |
| Launch Date: | | Security Office: | Smith, Sally |
| History Log: | View History Log | | |

After selecting the **Recalculation** option, the name of the Risk Assessment Coordinator displays.

10. Choose the **Yes** radio button next to **Launch Assessment** to launch the assessment, and then click **Save and Close**.

Location Assessment: 209090

0 of 35 Completed | Options ▾

This questionnaire is in a Development status. It is not licensed for Production.

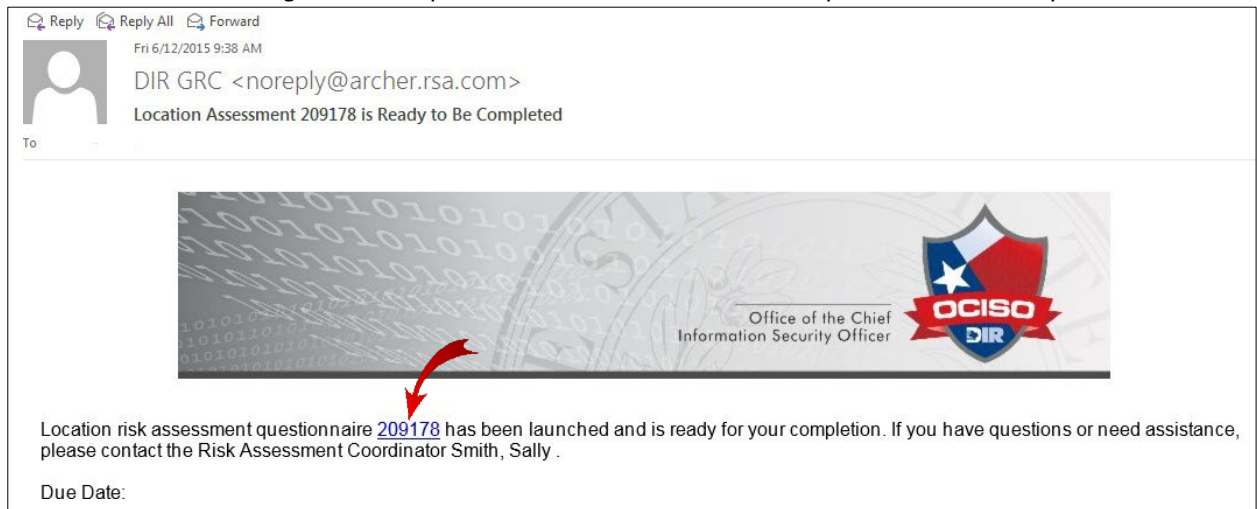
► Instructions

General Information

| | | | |
|------------------------------|---|----------------------------|------------------------|
| Questionnaire ID: | 209090 | Overall Assessment Status: | In Process by Assessor |
| * Location: | Archer Central Datacenter | Progress %: | 0.00 % |
| Organization Name: | State of Texas | Due Date: | 6/17/2015 |
| Risk Assessment Coordinator: | Smith, Sally | * Assessor: | Smith, Sally |
| Launch Assessment: | <input checked="" type="radio"/> Yes <input type="radio"/> No | Reviewer: | |
| Launch Date: | 6/3/2015 | * Security Office: | Smith, Sally |
| History Log: | View History Log | | |

Save and Close Save and Continue Cancel

The Assessor will receive an email with a link to the questionnaire indicating that they must complete an assessment. Selecting the link requires them to authenticate. The questionnaire will open.



Activity 3c: Create a Network Assessment Risk Assessment Coordinator Activity

Network Assessment(s) Section

Once the network has been associated to the RAU, you can add the assessment questionnaire.

1. To associate an existing questionnaire to the RAU, click **Lookup** in the **Network Assessment(s)** section.

| Network Information | | | | | | Add New Lookup |
|---------------------|-------------------|---------------|-------------------------------|-------------------|-------------------------|------------------|
| Network Name | Organization Name | Network Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type | |
| No Records Found | | | | | | |

| Network Assessment(s) | | | | | | | | Add New Lookup |
|-----------------------|---------|-------------|----------|------------|---------------------------|---------------|---------------|------------------|
| Questionnaire ID | Network | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk | |
| No Records Found | | | | | | | | |

The following screen displays.

| Questionnaire ID | Network | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
|---------------------------------|---------------------|-------------|--------------|------------|----------------------------------|---------------|---------------|
| <input type="checkbox"/> 208520 | Central Network | | Smith, Sally | 100.00 % | Findings Approved | Low | Low |
| <input type="checkbox"/> 208733 | Jean's Test Network | | | 100.00 % | Finding(s) In Process by Assesor | Low | Low |
| <input type="checkbox"/> 208844 | Jean's Test Network | | | 0.00 % | In Process by Assessor | Not Rated | Not Rated |

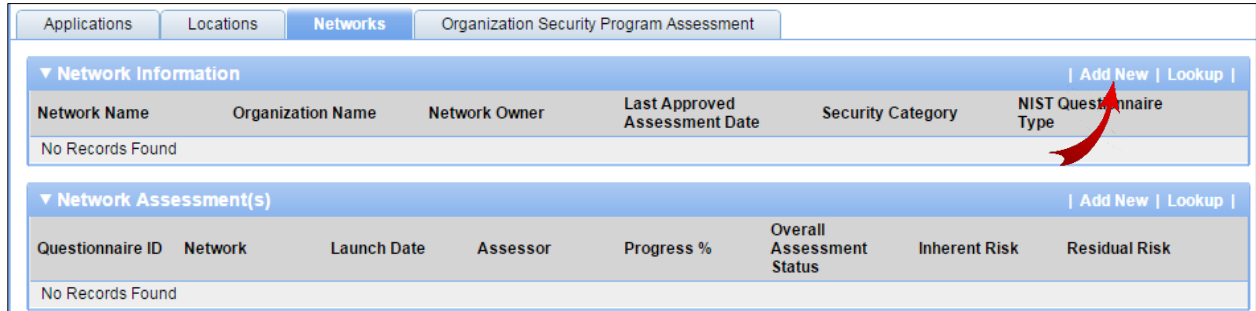
2. Select the checkbox next to the questionnaire you want to include, and then click **OK** to return to the RAU screen.

| Questionnaire ID | Network | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
|--|---------------------|-------------|--------------|------------|----------------------------------|---------------|---------------|
| <input checked="" type="checkbox"/> 208520 | Central Network | | Smith, Sally | 100.00 % | Findings Approved | Low | Low |
| <input type="checkbox"/> 208733 | Jean's Test Network | | | 100.00 % | Finding(s) In Process by Assesor | Low | Low |
| <input type="checkbox"/> 208844 | Jean's Test Network | | | 0.00 % | In Process by Assessor | Not Rated | Not Rated |

3. Click **Apply** to save your work and continue updating.

Note: Clicking **Save** will save and exit from the screen.

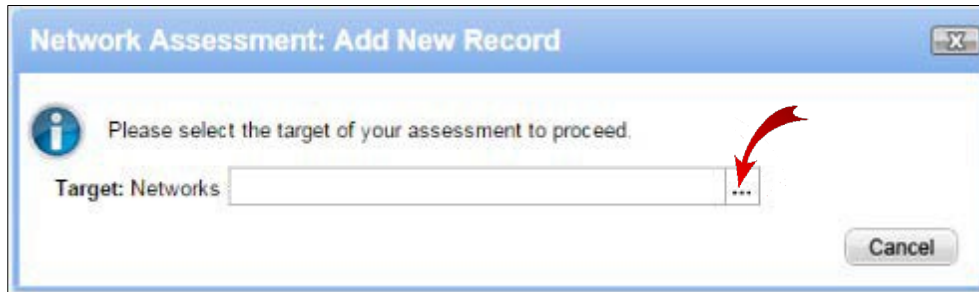
4. If the questionnaire is not already stored in SPECTRIM, click **Add New**.



| Applications | | Locations | | Networks | | Organization Security Program Assessment | |
|-------------------------|-------------------|---------------|-------------------------------|-------------------|---------------------------|--|---------------|
| ▼ Network Information | | | | | | Add New Lookup | |
| Network Name | Organization Name | Network Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type | | |
| No Records Found | | | | | | | |
| ▼ Network Assessment(s) | | | | | | Add New Lookup | |
| Questionnaire ID | Network | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
| No Records Found | | | | | | | |

The **Network Assessment: Add New Record** screen displays.

5. Click the ellipses and select the appropriate network to associate to the questionnaire.



Network Assessment: Add New Record

i Please select the target of your assessment to proceed.

Target: Networks ...

Cancel

6. Click **Apply**.

The *Network Assessment* screen displays.

Network Assessment: 209177

0 of 38 Completed | Options

This questionnaire is in a Development status. It is not licensed for Production.

► **Instructions**

General Information

| | | | |
|------------------------------|--|----------------------------|---------------------------------|
| Questionnaire ID: | 209177 | Overall Assessment Status: | In Process by Assessor |
| * Network: | Central Network | Progress %: | 0.00 % |
| Organization Name: | State Agency | Due Date: | <input type="text"/> [Calendar] |
| Risk Assessment Coordinator: | | * Assessor: | <input type="text"/> ... |
| Launch Assessment: | <input type="radio"/> Yes <input type="radio"/> No | Reviewer: | <input type="text"/> ... |
| Launch Date: | <input type="text"/> [Calendar] | * Security Office: | <input type="text"/> ... |
| History Log: | View History Log | | |

▼ **Comments**

| Question Name | Submitter | Date | Comment | Attachment |
|------------------|-----------|------|---------|------------|
| No Records Found | | | | |

General Information Section

Note: Red asterisks denote required fields.

- *Questionnaire ID:* Automatically generated by SPECTRIM.
- *Overall Status:* Automatically populated by SPECTRIM, as is **Organization Name*, **Location*, and *Progress*.
- Note that the *Risk Assessment Coordinator* fields is blank. Once you save this questionnaire and then save the RAU, the field will be populated. It is important to make sure this happens so you know that the questionnaire is linked to the RAU.
- *Due Date:* Enter the date the assessment questionnaire is due.
- **Assessor:* Select an assessor to answer the questions.
- *Reviewer:* Select a reviewer to review the answers (optional).
- **Security Office:* Select a member of the Security Office to review the assessment.
- *Launch Assessment:* Do not launch the assessment until the RAU has been saved.
- *Launch Date:* SPECTRIM will automatically populate this field.
- *History Log:* Shows a log of all actions taken on this questionnaire.

Comments Section

- *Comments:* Displays all comments attached to a question on the assessment as it is being processed.

7. Click **Save and Close** to return to the RAU record.
8. Click **Apply** to save your work and continue updating.

Note: Clicking **Save** will save and exit from the screen.

9. When you next open the assessment questionnaire, you may see the following text at the top of the screen:

“This record may not be up to date. If the Recalculation button is available, click it to refresh the record.”

Click the **Options** dropdown to expose the **Recalculation** option and select it.

Note: The **Risk Assessment Coordinator** field is blank.

| General Information | | | |
|------------------------------|---------------------------------|----------------------------|------------------------------|
| Questionnaire ID: | 209093 | Overall Assessment Status: | In Process by Assessor |
| Network: | Central Network | Progress %: | 0.00 % |
| Organization Name: | State Agency | Due Date: | 6/17/2015 |
| Risk Assessment Coordinator: | | Assessor: | Smith, Sally |
| Launch Assessment: | | Reviewer: | |
| Launch Date: | | Security Office: | Smith, Sally |

*After selecting the **Recalculation** option, the name of the Risk Assessment Coordinator displays.*

- Choose the **Yes** radio button next to **Launch Assessment** to launch the assessment, and then click **Save and Close**.

Network Assessment: 209093

0 of 38 Completed | Options ▾

This questionnaire is in a Development status. It is not licensed for Production.

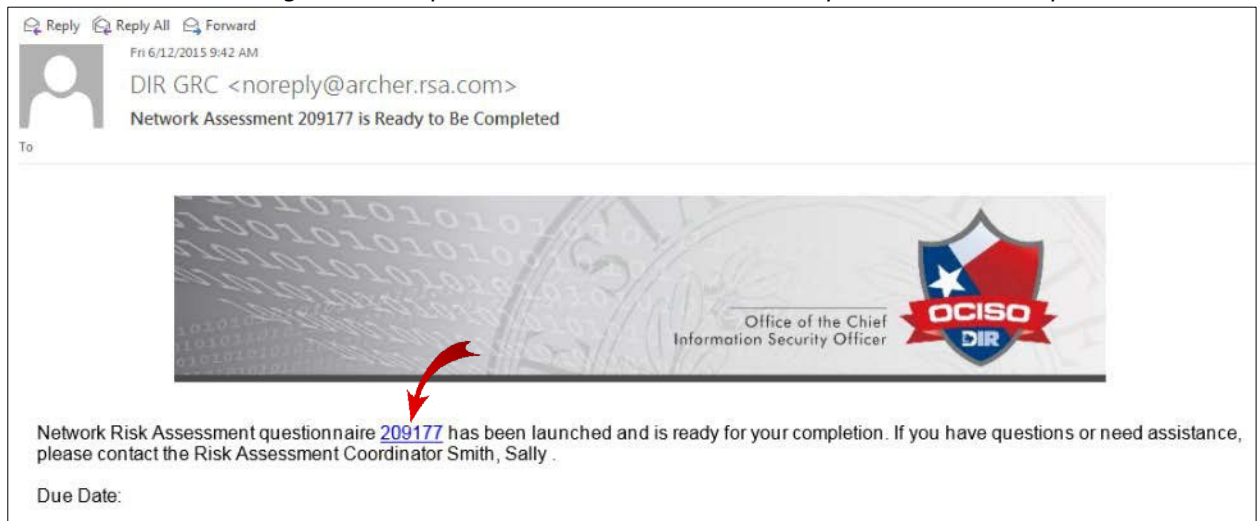
► Instructions

General Information

| | | | |
|------------------------------|---|----------------------------|------------------------|
| Questionnaire ID: | 209093 | Overall Assessment Status: | In Process by Assessor |
| * Network: | Central Network | Progress %: | 0.00 % |
| Organization Name: | State Agency | Due Date: | 6/17/2015 |
| Risk Assessment Coordinator: | Smith, Sally | * Assessor: | Smith, Sally |
| Launch Assessment: | <input checked="" type="radio"/> Yes <input type="radio"/> No | Reviewer: | |
| Launch Date: | 6/3/2015 | * Security Office: | Smith, Sally |
| History Log: | View History Log | | |

Save and Close Save and Continue Cancel

The Assessor will receive an email with a link to the questionnaire indicating that they must complete an assessment. Selecting the link requires them to authenticate. The questionnaire will open.

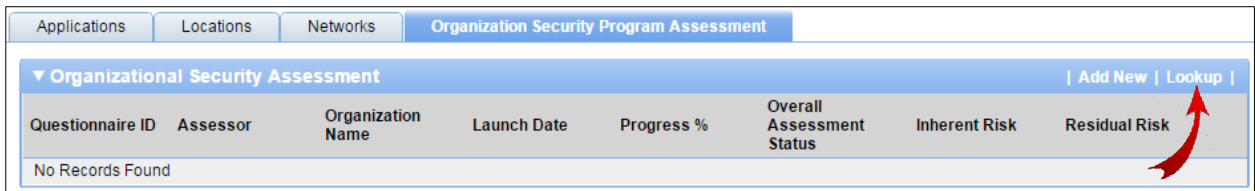


Activity 3d: Create an Organization Security Program Assessment
Risk Assessment Coordinator Activity

Organizational Security Assessment Section

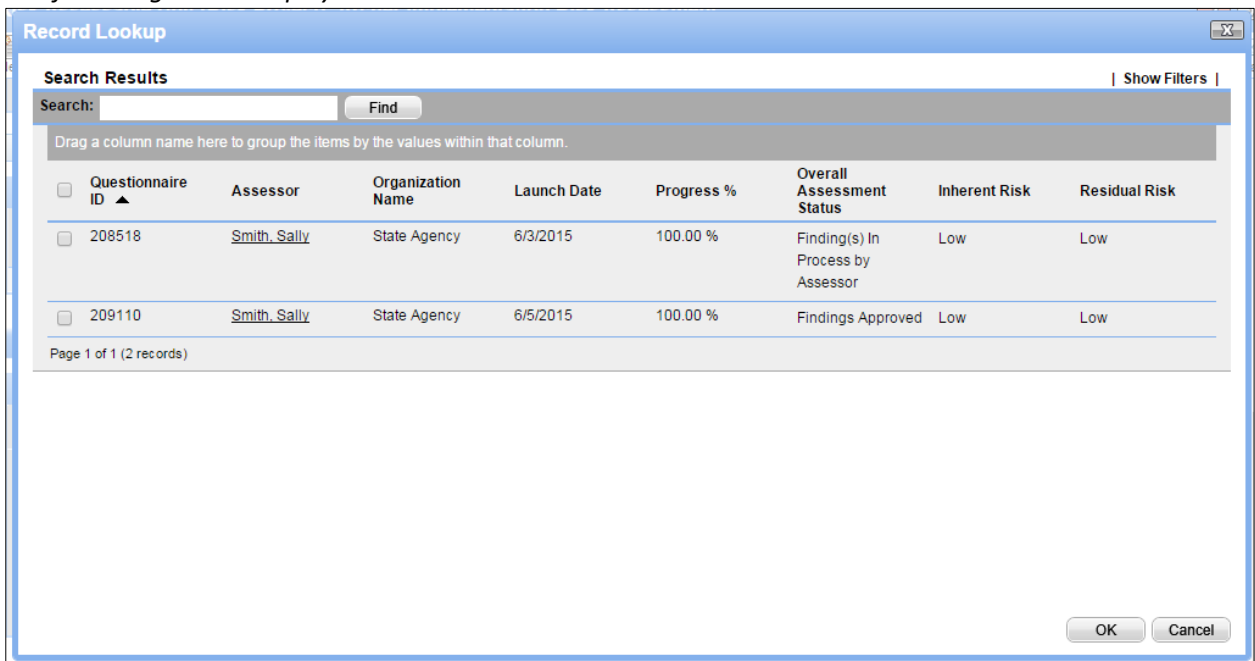
Once the network has been associated to the RAU, you can add the Assessment Questionnaire.

1. To associate an existing questionnaire to the RAU, click **Lookup** in the **Network Assessment(s)** section.



The screenshot shows a software interface with a tabbed menu at the top containing 'Applications', 'Locations', 'Networks', and 'Organization Security Program Assessment'. Below the tabs is a header for 'Organizational Security Assessment' with 'Add New' and 'Lookup' buttons. A table below the header has columns for 'Questionnaire ID', 'Assessor', 'Organization Name', 'Launch Date', 'Progress %', 'Overall Assessment Status', 'Inherent Risk', and 'Residual Risk'. The table currently shows 'No Records Found'. A red arrow points to the 'Lookup' button.

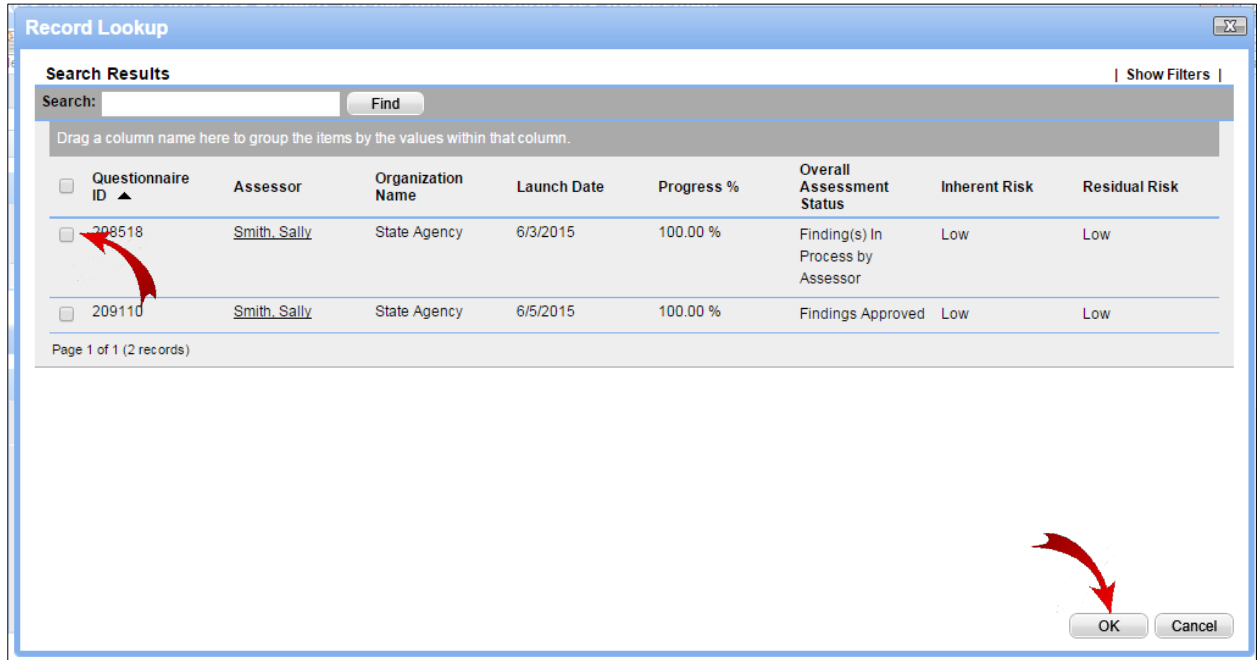
The following screen displays.



The screenshot shows a 'Record Lookup' dialog box with a search bar and a 'Find' button. Below the search bar is a table with search results. The table has columns for 'Questionnaire ID', 'Assessor', 'Organization Name', 'Launch Date', 'Progress %', 'Overall Assessment Status', 'Inherent Risk', and 'Residual Risk'. There are two records displayed. The first record has ID 208518, Assessor Smith, Sally, Organization Name State Agency, Launch Date 6/3/2015, Progress % 100.00 %, Overall Assessment Status Finding(s) In Process by Assessor, Inherent Risk Low, and Residual Risk Low. The second record has ID 209110, Assessor Smith, Sally, Organization Name State Agency, Launch Date 6/5/2015, Progress % 100.00 %, Overall Assessment Status Findings Approved, Inherent Risk Low, and Residual Risk Low. The dialog box also includes 'OK' and 'Cancel' buttons at the bottom right.

| Questionnaire ID | Assessor | Organization Name | Launch Date | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
|------------------|--------------|-------------------|-------------|------------|-----------------------------------|---------------|---------------|
| 208518 | Smith, Sally | State Agency | 6/3/2015 | 100.00 % | Finding(s) In Process by Assessor | Low | Low |
| 209110 | Smith, Sally | State Agency | 6/5/2015 | 100.00 % | Findings Approved | Low | Low |

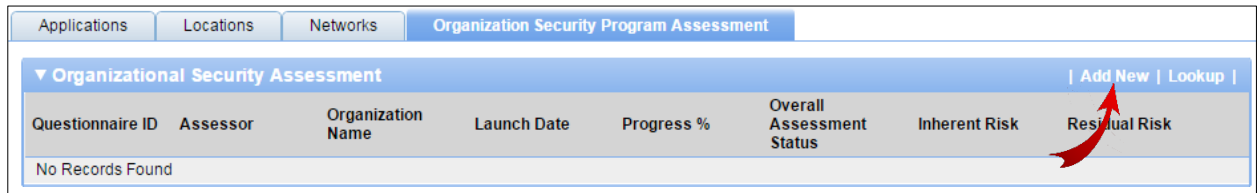
2. Select the checkbox next to the questionnaire you want to include, and then click **OK** to return to the RAU screen.



3. Click **Apply** to save your work and continue updating.

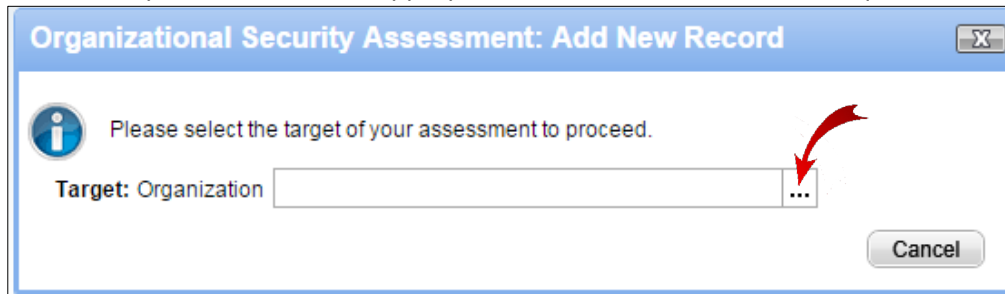
Note: Clicking **Save** will save and exit from the screen.

4. If the questionnaire is not already stored in SPECTRIM, click **Add New**.



The **Organizational Security Assessment: Add New Record** screen displays.

5. Click the ellipses and select the appropriate network to associate to the questionnaire.



6. Click **Apply**.

The *Organizational Security Assessment* screen displays.

| General Information | | | |
|------------------------------|--|----------------------------|--------------------------|
| Questionnaire ID: | 209115 | Overall Assessment Status: | In Process by Assessor |
| * Organization: | Q | Organization Name: | State Agency |
| Risk Assessment Coordinator: | | Progress %: | 0.00 % |
| Launch Assessment: | <input type="radio"/> Yes <input type="radio"/> No | Due Date: | <input type="text"/> |
| Launch Date: | <input type="text"/> | * Assessor: | <input type="text"/> ... |
| History Log: | View History Log | Reviewer: | <input type="text"/> ... |
| | | * Security Office: | <input type="text"/> ... |

| Question Name | Submitter | Date | Comment | Attachment |
|------------------|-----------|------|---------|------------|
| No Records Found | | | | |

General Information Section

Note: Red asterisks denote required fields.

- *Questionnaire ID:* Automatically generated by SPECTRIM.
- *Overall Status:* Automatically populated by SPECTRIM, as is * *Organization, Organization Name, Network, and Progress.*
- **Note:** The *Risk Assessment Coordinator* field is blank. Once you save this questionnaire and then save the RAU, the field will be populated. It is important to make sure this happens so you know that the questionnaire is linked to the RAU.
- *Due Date:* Enter the date the assessment questionnaire is due.
- * *Assessor:* Select an assessor to answer the questions.
- *Reviewer:* Select a reviewer to review the answers (optional).
- * *Security Office:* Select a member of the Security Office to review the assessment.
- *Launch Assessment:* Do not launch the assessment until the RAU has been saved.
- *Launch Date:* SPECTRIM will automatically populate this field.
- *History Log:* Shows a log of all actions taken on this questionnaire.

Comments Section

- *Comments:* Displays all comments attached to a question on the assessment as it is being processed.

7. Click **Save and Close** to return to the RAU record.
8. Click **Apply** to save your work and continue updating.

Note: Clicking **Save** will save and exit from the screen.

9. When you next open the assessment questionnaire, you may see the following text at the top of the screen:

“This record may not be up to date. If the Recalculation button is available, click it to refresh the record.”

Click the **Options** dropdown to expose the **Recalculation** option and select it.

Note: The **Risk Assessment Coordinator** field is blank.

| Organizational Security Assessment: 209115 | | | |
|--|----------------------------------|----------------------------|------------------------------|
| 0 of 104 Completed | | Options ▾ | |
| This questionnaire is in a Development status. It is not licensed for Production. | | | |
| This record may not be up to date. If the Recalculation button is available, click it to refresh the record. | | | |
| ► Instructions | | | |
| General Information | | | |
| Questionnaire ID: | 209115 | Overall Assessment Status: | In Process by Assessor |
| Organization: | Q | Organization Name: | State Agency |
| Risk Assessment Coordinator: | | Progress %: | 0.00 % |
| Launch Assessment: | | Due Date: | 6/10/2015 |
| Launch Date: | | Assessor: | Smith, Sally |
| History Log: | View History Log | Reviewer: | |
| | | Security Office: | Smith, Sally |

After selecting the **Recalculation** option, the name of the Risk Assessment Coordinator displays.

10. Choose the **Yes** radio button next to **Launch Assessment** to launch the assessment, and then click **Save and Close**.

Organizational Security Assessment: 209115

0 of 104 Completed | Options

This questionnaire is in a Development status. It is not licensed for Production.

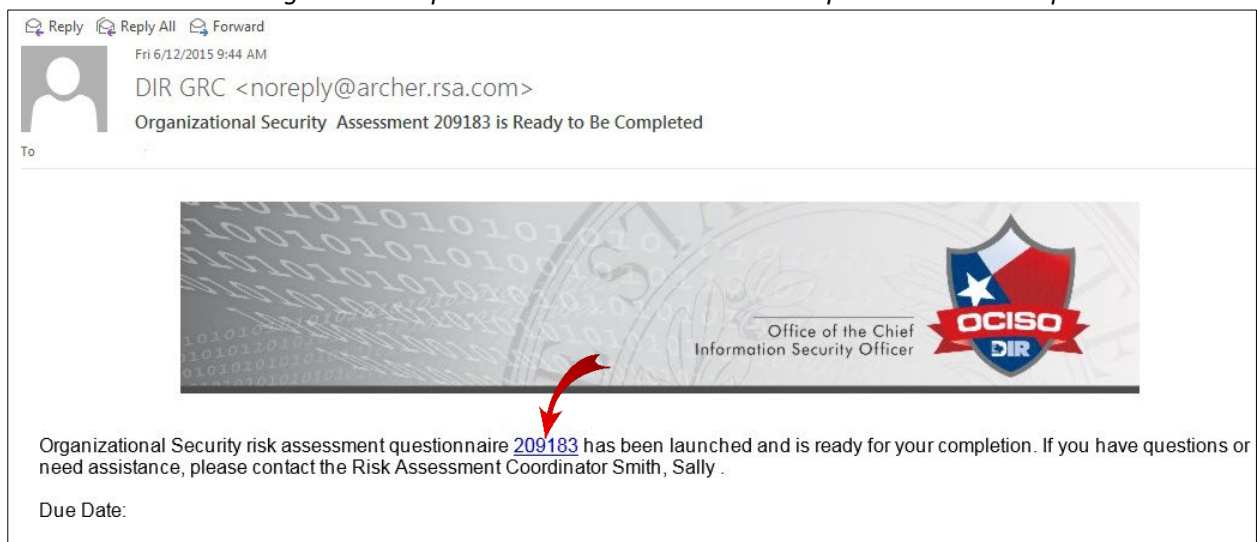
► Instructions

General Information

| | | | |
|------------------------------|---|----------------------------|------------------------|
| Questionnaire ID: | 209115 | Overall Assessment Status: | In Process by Assessor |
| * Organization: | Q | Organization Name: | State Agency |
| Risk Assessment Coordinator: | Smith, Sally | Progress %: | 0.00 % |
| Launch Assessment: | <input checked="" type="radio"/> Yes <input type="radio"/> No | Due Date: | 6/10/2015 |
| Launch Date: | 6/5/2015 | * Assessor: | Smith, Sally |
| History Log: | View History Log | Reviewer: | |
| | | * Security Office: | Smith, Sally |

Save and Close Save and Continue Cancel

The Assessor will receive an email with a link to the questionnaire indicating that they must complete an assessment. Selecting the link requires them to authenticate. The questionnaire will open.



6.0 Launching the Assessment

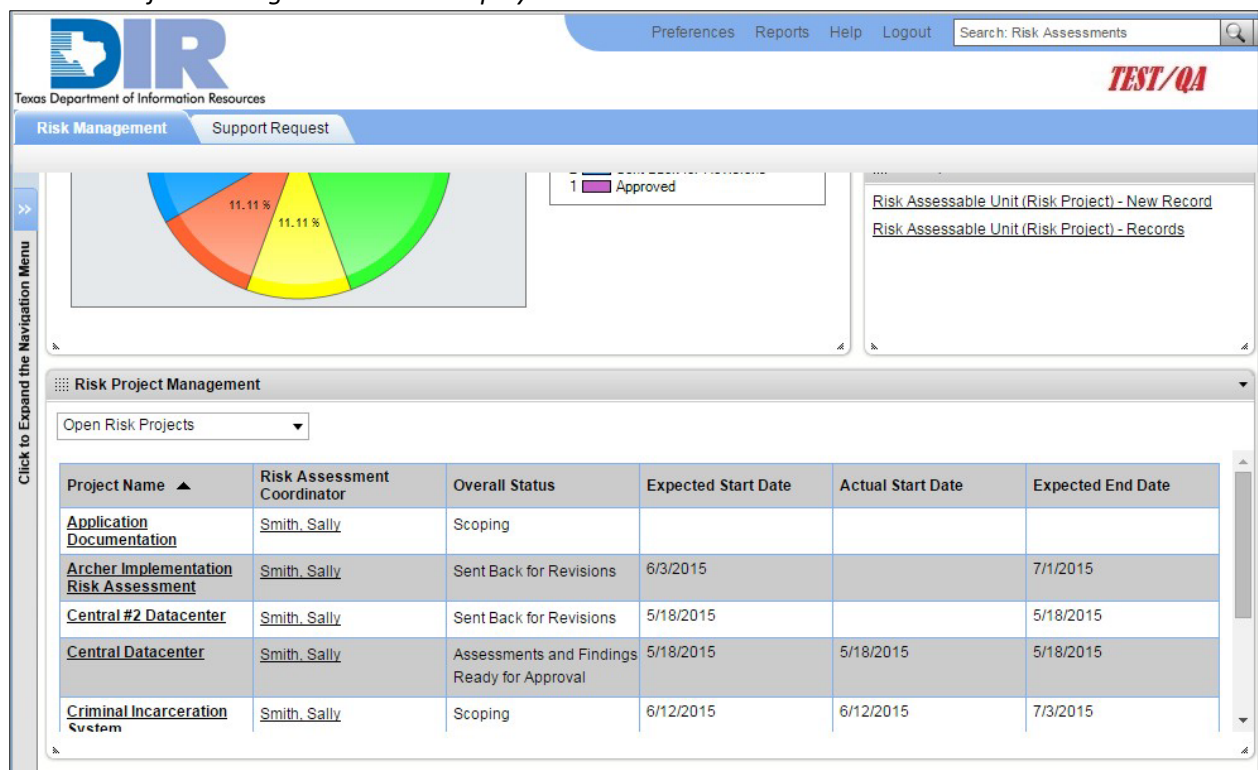
Activity 4: Save the Risk Assessable Unit and Initiate Assessment Workflow

Risk Assessment Coordinator Activity

The fourth activity for the Risk Assessment Coordinator is to save the Risk Assessable Unit (RAU) and begin the SPECTRIM workflow. If all assessment components have been added for your RAU and each assessment component has an associated questionnaire that has been launched, your work in SPECTRIM should be complete. You can monitor the progress of the assessment by checking the Risk Project Management list on your SPECTRIM dashboard.

1. Log in to your SPECTRIM account. See 4.0 Logging into SPECTRIM on page 7 for instructions on how to log in to SPECTRIM.
2. Click the **Risk Management** tab to view the *Risk Management Summary*.

The Risk Project Management screen displays.



The screenshot displays the SPECTRIM Risk Project Management interface. At the top, there is a navigation bar with the DIR logo (Texas Department of Information Resources) and a search bar containing "Risk Assessments". Below the navigation bar, there are tabs for "Risk Management" and "Support Request". The main content area features a pie chart with two segments labeled "11.11%" and a legend indicating "1 Approved". To the right of the pie chart, there are links for "Risk Assessable Unit (Risk Project) - New Record" and "Risk Assessable Unit (Risk Project) - Records". Below this, there is a section titled "Risk Project Management" with a dropdown menu for "Open Risk Projects". The main part of the screen is a table with the following data:

| Project Name ▲ | Risk Assessment Coordinator | Overall Status | Expected Start Date | Actual Start Date | Expected End Date |
|---|------------------------------|---|---------------------|-------------------|-------------------|
| Application Documentation | Smith, Sally | Scoping | | | |
| Archer Implementation Risk Assessment | Smith, Sally | Sent Back for Revisions | 6/3/2015 | | 7/1/2015 |
| Central #2 Datacenter | Smith, Sally | Sent Back for Revisions | 5/18/2015 | | 5/18/2015 |
| Central Datacenter | Smith, Sally | Assessments and Findings Ready for Approval | 5/18/2015 | 5/18/2015 | 5/18/2015 |
| Criminal Incarceration System | Smith, Sally | Scoping | 6/12/2015 | 6/12/2015 | 7/3/2015 |

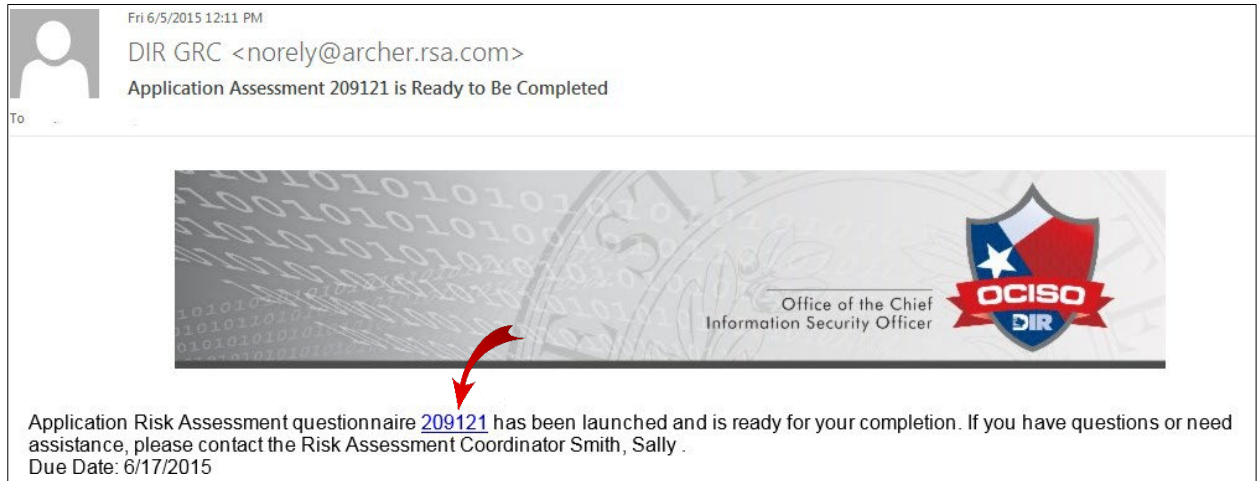
7.0 Completing the Assessment

Activity 5: Complete the Assessment Questionnaire

Assessor Activity

You will receive an email from <DIR GRC noreply@Archerirm.us> notifying you that an assessment questionnaire has been assigned to you.

1. When you receive the email, click the questionnaire number link in the email to complete the questionnaire.



You will be directed to a login page.

2. Log in to your SPECTRIM account. See 4.0 Logging into SPECTRIM for instructions on how to log in.

The assessment questionnaire opens.

Comments Section

- *Comments:* If comments are provided, they will display here.

3. Click the **Edit** button to complete the questionnaire. Please refer to the following descriptions when choosing your responses.

Possible Responses

- *Implemented:* The full extent of the requirement has been implemented, documented, and communicated and is consistently applied.
- *Partially Implemented:* Some of the characteristics of the control requirement are being performed but may not be documented, communicated, nor consistently applied.
- *Not Implemented:* The control requirement is not currently being performed or has not been implemented.
- *Unknown:* It cannot be determined whether the control requirement is being performed or implemented.
- *N/A:* The specific control requirement is not applicable to the component being assessed.

Help Text

Certain questions will contain help text that might assist you in answering the question. Help text is denoted by the blue and white question mark icon.

or



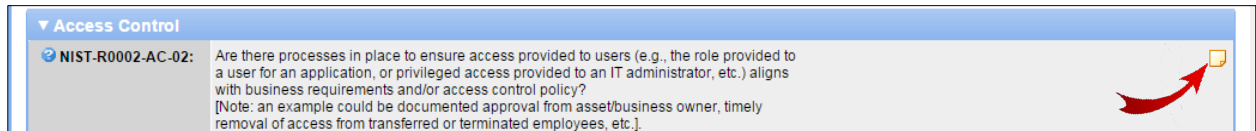
The screenshot shows a list of four questions under the 'Access Control' section. Each question has a blue and white question mark icon to its left, indicating that help text is available. A red arrow points to the first question's icon. The questions are:

- NIST-R0002-AC-02:** Are there processes in place to ensure access provided to users (e.g., the role provided to a user for an application, or privileged access provided to an IT administrator, etc.) aligns with business requirements and/or access control policy? [Note: an example could be documented approval from asset/business owner, timely removal of access from transferred or terminated employees, etc.]
- NIST-R0003-AC-03.02:** Are information systems (Application Assessments; operating systems; Network Assessment devices; databases; etc.) configured and access enforcement mechanisms employed per approved policy to provide protection from unauthorized access by malicious users; software or systems?
- NIST-R0007-AC-07:** Have you implemented procedures and controls to lock user access to information resources after a defined number of unsuccessful login attempts?
- NIST-R0008-AC-08:** Do organizational or departmental information systems display an approved system use notification message or banner before granting access to the information system?

At the bottom of the list are 'Edit' and 'Cancel' buttons.

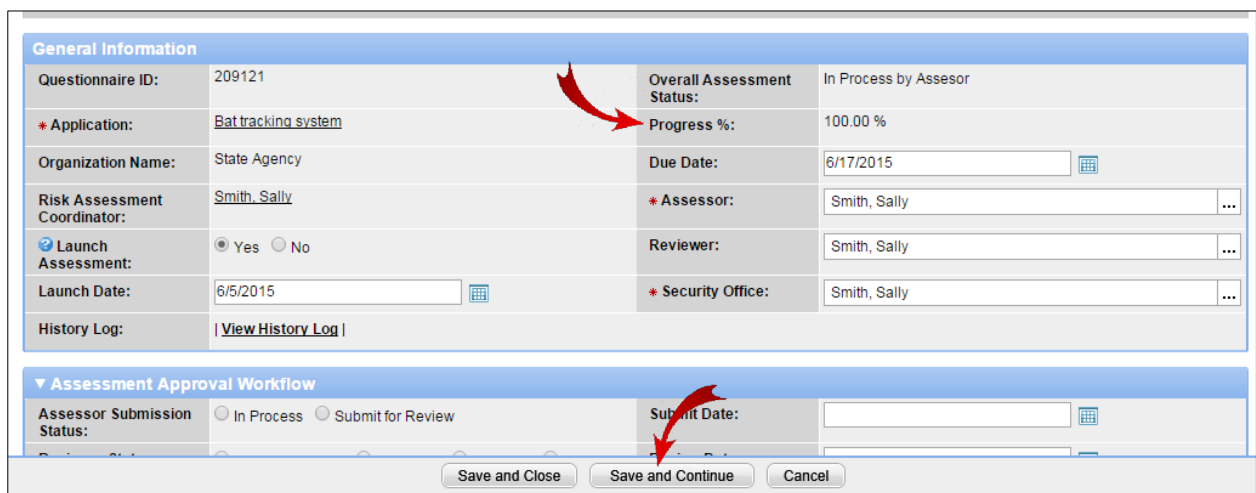
Comments

Click the yellow sticky icon to the side to insert comments. You may use the comment box to refer to specific organizational policies, procedures, and standards; to describe the status of a *partially implemented* response; or to explain a *not implemented* or *unknown* response.



This screenshot is similar to the previous one, but a red arrow points to a yellow sticky icon located to the right of the first question's text.

- Once you answer all of the questions, the *Progress %* field will change to 100%. If it does not show 100%, go back and answer the questions you missed. Once you finish answering all questions, click the **Save and Continue** button.



The screenshot shows two sections of the interface:

- General Information:** A table with fields for Questionnaire ID (209121), Application (Bat tracking system), Organization Name (State Agency), Risk Assessment Coordinator (Smith, Sally), Launch Assessment (Yes selected), Launch Date (6/5/2015), and History Log (View History Log). On the right, Overall Assessment Status is 'In Process by Assesor', Progress % is '100.00 %', Due Date is '6/17/2015', Assessor is 'Smith, Sally', Reviewer is 'Smith, Sally', and Security Office is 'Smith, Sally'. A red arrow points to the Progress % field.
- Assessment Approval Workflow:** Shows Assessor Submission Status (In Process selected), Submit Date (empty), and buttons for 'Save and Close', 'Save and Continue', and 'Cancel'. A red arrow points to the 'Save and Continue' button.

This action will take you to the top of the Questionnaire screen.

- If the *Progress %* field shows 100%, you will see the **Assessment Approval Workflow** box.

| General Information | | | |
|------------------------------|---|----------------------------|----------------------------------|
| Questionnaire ID: | 209121 | Overall Assessment Status: | In Process by Assesor |
| * Application: | Bat tracking system | Progress %: | 100.00 % |
| Organization Name: | State Agency | Due Date: | 6/17/2015 |
| Risk Assessment Coordinator: | Smith, Sally | * Assessor: | Smith, Sally ... |
| Launch Assessment: | <input checked="" type="radio"/> Yes <input type="radio"/> No | Reviewer: | Smith, Sally ... |
| Launch Date: | 6/5/2015 | * Security Office: | Smith, Sally ... |
| History Log: | View History Log | | |

| Assessment Approval Workflow | |
|------------------------------|--|
| Assessor Submission Status: | <input type="radio"/> In Process <input type="radio"/> Submit for Review |
| Submit Date: | |

Choose the **Submit for Review** radio button in the *Assessor Submission Status* section.

| Assessment Approval Workflow | |
|------------------------------|---|
| Assessor Submission Status: | <input type="radio"/> In Process <input checked="" type="radio"/> Submit for Review |
| Submit Date: | |

*This action will route the questionnaire to the Reviewer, if one is selected, or the Security Office if not. If routed to the Reviewer, the RAU will show the status as **Awaiting Review by Reviewer**.*

| Applications | | | | | | Add New Lookup |
|-------------------------------------|-------------------|------------------------------|-------------------------------|-------------------|-------------------------|----------------------------------|
| Information System Name | Organization Name | Application Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type | |
| Bat tracking system | State Agency | Smith, Sally | 6/5/2015 | Moderate | NIST Low | <input type="button" value="X"/> |

| Application Assessment(s) | | | | | | | | Add New Lookup |
|---------------------------|-------------------------------------|-------------|------------------------------|------------|-----------------------------|---------------|---------------|----------------------------------|
| Questionnaire ID | Application | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk | |
| 209121 | Bat tracking system | 6/5/2015 | Smith, Sally | 100.00 % | Awaiting Review by Reviewer | Low | Low | <input type="button" value="X"/> |

8.0 Reviewing the Assessment

Activity 6: Approve or Reject the Questionnaire

Reviewer Activity

You will receive an email from <DIR GRC noreply@Archerirm.us> notifying you that an assessment questionnaire has been assigned to you for review.

1. Click the link in the email to review the questionnaire.



You will be directed to a login page.

2. Log in to your SPECTRIM account. See 4.0 Logging into SPECTRIM on page 7 for instructions on how to log in.

The completed assessment questionnaire opens.

3. Scroll down to see the following portion of screen.

| ▼ Comments | | | | | |
|----------------------|------------------|------------------------------|----------|---------------------------------------|------------|
| | Question Name | Submitter | Date | Comment | Attachment |
| View | NIST-R0174-CM-10 | Smith, Sally | 6/5/2015 | I was unable to answer this question. | |

| ▼ Access Control | | | | | |
|------------------------|--|--|--|-------------|--|
| ☑ NIST-R0002-AC-02: | Are there processes in place to ensure access provided to users (e.g., the role provided to a user for an application, or privileged access provided to an IT administrator, etc.) aligns with business requirements and/or access control policy? [Note: an example could be documented approval from asset/business owner, timely removal of access from transferred or terminated employees, etc.] | | | Implemented | |
| ☑ NIST-R0003-AC-03.02: | Are information systems (Application Assessments;operating systems;Network Assessment devices;databases;etc.) configured and access enforcement mechanisms employed per approved policy to provide protection from unauthorized access by malicious users;software or systems? | | | Implemented | |
| ☑ NIST-R0007-AC-07: | Have you implemented procedures and controls to lock user access to information resources after a defined number of unsuccessful login attempts? | | | Implemented | |

This screen shows the responses to the questions given by the assessor.

Possible Responses

- *Implemented*: The full extent of the requirement has been implemented, documented, and communicated and is consistently applied.
- *Partially Implemented*: Some of the characteristics of the control requirement are being performed but may not be documented, communicated, nor consistently applied.
- *Not Implemented*: The control requirement is not currently being performed or has not been implemented.
- *Unknown*: It cannot be determined whether the control requirement is being performed or implemented.
- *N/A*: The specific control requirement is not applicable to the component being assessed.

Note: Each question has a comment box that you may use to document or clarify responses.

4. After reviewing all questions, click **Edit** at the bottom of the screen to return to the top of the record as shown below.

| General Information | | | |
|------------------------------|-------------------------------------|----------------------------|------------------------------|
| Questionnaire ID: | 209121 | Overall Assessment Status: | Awaiting Review by Reviewer |
| * Application: | Bat tracking system | Progress %: | 100.00 % |
| Organization Name: | State Agency | Due Date: | 6/17/2015 |
| Risk Assessment Coordinator: | Smith, Sally | * Assessor: | Smith, Sally |
| Launch Assessment: | Yes | Reviewer: | Smith, Sally |
| Launch Date: | 6/5/2015 | * Security Office: | Smith, Sally |
| History Log: | View History Log | | |

| Assessment Approval Workflow | | | |
|------------------------------|--|--------------|---------------------------------------|
| Assessor Submission Status: | <input type="radio"/> In Process <input checked="" type="radio"/> Submit for Review | Submit Date: | <input type="text" value="6/5/2015"/> |
| Reviewer Status: | <input checked="" type="radio"/> Awaiting Review <input type="radio"/> Approved <input type="radio"/> Rejected <input type="radio"/> N/A | Review Date: | <input type="text"/> |
| Reviewer Notes: | | | |

5. Choose the appropriate radio button in the *Reviewer Status*: section to **Approve** or **Reject** the questionnaire.

| Assessment Approval Workflow | | | |
|------------------------------|--|--------------|---------------------------------------|
| Assessor Submission Status: | <input type="radio"/> In Process <input checked="" type="radio"/> Submit for Review | Submit Date: | <input type="text" value="6/5/2015"/> |
| Reviewer Status: | <input checked="" type="radio"/> Awaiting Review <input type="radio"/> Approved <input type="radio"/> Rejected <input type="radio"/> N/A | Review Date: | <input type="text"/> |
| Reviewer Notes: | | | |

Note: Clicking *Rejected* routes the assessment questionnaire back to the assessor. Clicking *Approved* routes it to the Information Security Group. If no Reviewer is selected, *N/A* will automatically be selected.

6. If applicable, enter notes in the *Reviewer Notes* field.

| Assessment Approval Workflow | | | |
|------------------------------|--|--------------|---------------------------------------|
| Assessor Submission Status: | <input type="radio"/> In Process <input checked="" type="radio"/> Submit for Review | Submit Date: | <input type="text" value="6/5/2015"/> |
| Reviewer Status: | <input checked="" type="radio"/> Awaiting Review <input type="radio"/> Approved <input type="radio"/> Rejected <input type="radio"/> N/A | Review Date: | <input type="text"/> |
| Reviewer Notes: | | | |

Now the RAU shows that the assessment questionnaire is **Awaiting Review by Security Office**.

| Applications | | | | | | Add New Lookup | |
|-------------------------------------|-------------------|------------------------------|-------------------------------|-------------------|-------------------------|------------------|--|
| Information System Name | Organization Name | Application Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type | | |
| Bat tracking system | State Agency | Smith, Sally | 6/5/2015 | Moderate | NIST Low | | |

| Application Assessment(s) | | | | | | | | Add New Lookup | |
|---------------------------|-------------------------------------|-------------|------------------------------|------------|------------------------------------|---------------|---------------|------------------|--|
| Questionnaire ID | Application | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk | | |
| 209121 | Bat tracking system | 6/5/2015 | Smith, Sally | 100.00 % | Awaiting Review by Security Office | Low | Low | | |

7. Click **Apply** to save your work and continue updating.

Note: Clicking **Save** will save and exit from the screen.

Activity 7: Approve or Reject the Questionnaire

Security Office Activity

You will receive an email from <DIR GRC noreply@Archerirm.us> notifying you that an assessment questionnaire has been assigned to you for review.

1. Click the link in the email to review the questionnaire.



You will be directed to a login page.

2. Log in to your SPECTRIM account. See 4.0 Logging into SPECTRIM on page 7 for instructions on how to log in.

The completed assessment questionnaire opens.

3. Scroll down to see the following portion of screen.

| ▼ Comments | | | | | |
|----------------------|------------------|------------------------------|----------|---------------------------------------|------------|
| | Question Name | Submitter | Date | Comment | Attachment |
| View | NIST-R0174-CM-10 | Smith, Sally | 6/5/2015 | I was unable to answer this question. | |

| ▼ Access Control | | | | | |
|------------------------|--|--|--|-------------|---|
| 🔍 NIST-R0002-AC-02: | Are there processes in place to ensure access provided to users (e.g., the role provided to a user for an application, or privileged access provided to an IT administrator, etc.) aligns with business requirements and/or access control policy? [Note: an example could be documented approval from asset/business owner, timely removal of access from transferred or terminated employees, etc.] | | | Implemented | 📄 |
| 🔍 NIST-R0003-AC-03.02: | Are information systems (Application Assessments; operating systems; Network Assessment devices; databases; etc.) configured and access enforcement mechanisms employed per approved policy to provide protection from unauthorized access by malicious users; software or systems? | | | Implemented | 📄 |
| 🔍 NIST-R0007-AC-07: | Have you implemented procedures and controls to lock user access to information resources after a defined number of unsuccessful login attempts? | | | Implemented | 📄 |

This screen shows the responses to the questions given by the assessor and approved by the reviewer if selected.

Possible Responses

- *Implemented:* The full extent of the requirement has been implemented, documented, and communicated and is consistently applied.
- *Partially Implemented:* Some of the characteristics of the control requirement are being performed but may not be documented, communicated, nor consistently applied.
- *Not Implemented:* The control requirement is not currently being performed or has not been implemented.
- *Unknown:* It cannot be determined whether the control requirement is being performed or implemented.
- *N/A:* The specific control requirement is not applicable to the component being assessed.

Note: Each question has a comment box that you may use to document or clarify responses.

4. After reviewing all questions, click **Edit** to return to the top of the screen as shown below.

| Application Assessment(s): 209121 | | | |
|--|--|------------------------------|--------------|
| 43 of 43 Completed Opt | | | |
| This questionnaire is in a Development status. It is not licensed for Production. | | | |
| * Application: | Bat tracking system | Progress %: | 100.00 % |
| Organization Name: | State Agency | Due Date: | 6/17/2015 |
| Risk Assessment Coordinator: | Smith, Sally | * Assessor: | Smith, Sally |
| Launch Assessment: | <input checked="" type="radio"/> Yes <input type="radio"/> No | Reviewer: | Smith, Sally |
| Launch Date: | 6/5/2015 | * Security Office: | Smith, Sally |
| History Log: | View History Log | | |
| Assessment Approval Workflow | | | |
| Assessor Submission Status: | <input type="radio"/> In Process <input checked="" type="radio"/> Submit for Review | Submit Date: | 6/5/2015 |
| Reviewer Status: | <input type="radio"/> Awaiting Review <input checked="" type="radio"/> Approved <input type="radio"/> Rejected <input type="radio"/> N/A | Review Date: | 6/5/2015 |
| Reviewer Notes: | | | |
| Security Office Review Status: | <input checked="" type="radio"/> Awaiting Review <input type="radio"/> Approved <input type="radio"/> Rejected | Security Office Review Date: | 6/5/2015 |
| Security Office | | | |

5. Choose the appropriate radio button in the **Reviewer Status:** section to **Approve** or **Reject** the questionnaire.

| Assessment Approval Workflow | | | |
|------------------------------|--|--------------|----------|
| Assessor Submission Status: | <input type="radio"/> In Process <input checked="" type="radio"/> Submit for Review | Submit Date: | 6/5/2015 |
| Reviewer Status: | <input type="radio"/> Awaiting Review <input checked="" type="radio"/> Approved <input type="radio"/> Rejected <input type="radio"/> N/A | Review Date: | 6/5/2015 |
| Reviewer Notes: | | | |

Clicking *Rejected* routes the assessment questionnaire back to the assessor. Clicking *Approved* routes it to the Information Security Group. If there is no Reviewer, *N/A* will automatically be selected.

6. If applicable, enter notes in the *Reviewer Notes* field.

| ▼ Assessment Approval Workflow | | | |
|--------------------------------|--|--------------|----------|
| Assessor Submission Status: | <input type="radio"/> In Process <input checked="" type="radio"/> Submit for Review | Submit Date: | 6/5/2015 |
| Reviewer Status: | <input type="radio"/> Awaiting Review <input checked="" type="radio"/> Approved <input type="radio"/> Rejected <input type="radio"/> N/A | Review Date: | 6/5/2015 |
| Reviewer Notes: | | | |

Now the RAU shows that the assessment questionnaire as having findings in process by the Assessor.

| Applications | Locations | Networks | Organization Security Program Assessment | | | | |
|---|-------------------------------------|------------------------------|--|-------------------|-----------------------------------|---------------|---------------|
| ▼ Applications Add | | | | | | | |
| Information System Name | Organization Name | Application Owner | Last Approved Assessment Date | Security Category | NIST Questionnaire Type | | |
| Bat tracking system | State Agency | Smith, Sally | 6/5/2015 | Moderate | NIST Low | | |
| ▼ Application Assessment(s) | | | | | | | |
| Questionnaire ID | Application | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
| 209121 | Bat tracking system | 6/5/2015 | Smith, Sally | 100.00 % | Finding(s) In Process by Assessor | Low | Low |

7. Click **Apply** to save your work and continue updating.

Note: Clicking **Save** will save and exit from the screen.

9.0 Responding to Findings

Activity 8: Respond to Findings

Assessor Activity

You will receive an email from <DIR GRC noreply@Archerirm.us> notifying you that there are findings from the assessment that require you to review and determine whether you will remediate or accept the risk.

1. Click the questionnaire number link in the email to review the findings.



You will be directed to a login page.

2. Log in to your SPECTRIM account. See 4.0 Logging into SPECTRIM on page 7 for instructions on how to log in.

The completed assessment questionnaire opens.

3. Scroll down to see three new sections.

Note: These sections were previously hidden until findings were generated.

There is a section for sending the findings through workflow once all have been addressed. There is also a quantitative summary section showing inherent and residual risk scores.

When the findings are initially generated, the two scores are equal. As you determine which findings you plan to address and which you plan to accept the risk on, the residual risk score improves.

Note: The **Findings** section is collapsed.

- Click the arrow to expand the **Findings** section.

| ▼ Findings Approval Workflow | | | |
|-------------------------------------|--|-------------------------------|--|
| Assessor Finding Submission Status: | | Finding Submit Date: | |
| Reviewer Finding Approval Status: | | Reviewer Finding Review Date: | |
| Finding Reviewer Notes: | | | |

| Quantitative Summary | | | |
|----------------------|-------|----------------------|-------|
| Inherent Risk: | Low | Residual Risk: | Low |
| Inherent Risk Score: | 94.19 | Residual Risk Score: | 94.19 |

► Findings

The **Findings** section expands.

- Click the **Finding ID** link to address a finding.

| ▼ Findings | | | | | |
|-------------------------|--|------------|--------------------------|-------------|----------|
| Finding ID | Finding | Status | Category | Criticality | Response |
| FND-317 | The question: "Are changes to information systems (including those related to procedures;processes;system and service parameters) logged;assessed and authorized prior to implementation and | In Process | Configuration Management | | |

A screen similar to the following screen displays for each finding.

Findings: FND-317

New Copy Save Apply Edit Delete Related Recalculate Export Print

First Published: 6/5/2015 1:04 PM Last Updated: 6/5/2015 1:04 PM

► About

▼ General Information

| | | | |
|---------------|--------------------------|----------------|---|
| Finding ID: | FND-317 | Status: | In Process |
| Category: | Configuration Management | Target: | Applications: Bat tracking system |
| Criticality: | | Questionnaire: | Application Assessment: 209121 |
| Year: | 2015 | Source: | Risk |
| Finding Type: | Application | | |

Workflow and Description

▼ Workflow

| | | | |
|-----------|------------------------------|--------------------|-----------------|
| Assessor: | Smith, Sally | Submission Status: | In Process |
| | | Submit Date: | |
| | | Review Status: | Awaiting Review |
| | | Review Date: | |

General Information Section

Note: These fields are all automatically generated by SPECTRIM except for *Criticality*.

- *Finding ID:* Unique identifier for the finding.
- *Status:* Either *In Process* or *Closed*.
- *Category:* The NIST Category for the findings.
- *Target:* The section of the RAU that this finding is generated from.
- *Criticality:* Rate this finding High, Medium, or Low according to the level of risk this exposes your organization to.
- *Questionnaire:* The Questionnaire number which generated the finding.
- *Year:* Calendar year in which the finding was generated.
- *Source:* This will always show that the SPECTRIM Risk application is the source.
- *Finding Type:* This indicates the type of questionnaire that generated the finding. Possible types are Application, Location, Network, and Organizational Security Program.

Workflow Section

The Workflow section shows the assessor and status of the finding. These fields are automatically generated by SPECTRIM, so no action on your part is required.

Description Section

The following image shows the actual finding name that is automatically generated by SPECTRIM and the finding itself.

| ▼ Description | |
|------------------|---|
| Name: | Auto-Finding Generated: NIST-R0040-CM-04.01 |
| Finding: | The question: "Are changes to information systems (including those related to procedures;processes;system and service parameters) logged;assessed and authorized prior to implementation and reviewed against planned outcomes following implementation (including impact from an information security perspective)?" was answered incorrectly. Question: NIST-R0040-CM-04.01 Answer: Partially Implemented Question Risk Score: 0.5 |
| Response: | Assigned to: |

| ▼ Attachment(s) | | | |
|------------------|------|------|-------------|
| Name | Size | Type | Upload Date |
| No Records Found | | | |

► History Log

► Administration

- Click **Edit** to insert the criticality and indicate your response.

Findings: FND-317

New Copy Save Apply Edit Delete

Related Recalculate Export Print

First Published: 6/5/2015 1:04 PM Last Updated: 6/5/2015 1:04 PM

The **Description** and **Remediation** sections open for editing.

- Edit the fields as appropriate.

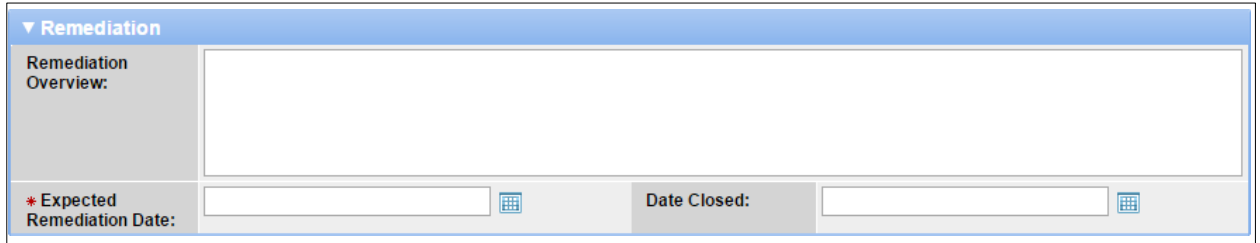
| ▼ Description | |
|--------------------|---|
| Name: | Auto-Finding Generated: NIST-R0040-CM-04.01 |
| Finding: | The question: "Are changes to information systems (including those related to procedures;processes;system and service parameters) logged;assessed and authorized prior to implementation and reviewed against planned outcomes following implementation (including impact from an information security perspective)?" was answered incorrectly. Question: NIST-R0040-CM-04.01 Answer: Partially Implemented Question Risk Score: 0.5 |
| * Response: | * Assigned to: |

Note: The *Name* and *Findings* fields are automatically generated by SPECTRIM. You can replace the text with your own if necessary.

Description Section

Note: Red asterisks denote required fields.

- ***Response:** If you select *Remediate Risk* as your response, a section titled **Remediation** will display.



▼ Remediation

Remediation Overview:

* Expected Remediation Date: 

Date Closed: 

If you select *Accept Risk* as your response, a section titled **Risk Acceptance** will display.



▼ Risk Acceptance

* Risk Acceptance Details:

- ***Assigned to:** Indicate the person whom you wish to address the finding. This person will receive a digest email at the end of the day indicating the findings that have been assigned to him/her.

Remediation Section

Note: Red asterisks denote required fields.

- **Remediation Overview:** Indicate recommended actions to address the finding. This can be entered by the assessor or by the person assigned to the finding.
- ***Expected Remediation Date:** Designate a deadline for the finding.
- **Date Closed:** Update this field when remediation activities are complete.

Risk Acceptance Section

- ***Risk Acceptance Details:** Document your reasons for accepting the risk.

Note: When you address findings, the questionnaire screen changes, indicating the criticality and recommended response as shown in the following image.



| ▼ Findings | | | | | |
|-------------------------|---|-----------------|--------------------------|-------------|----------------|
| Finding ID | Finding | Status | Category | Criticality | Response |
| FND-317 | The question: "Are changes to information systems (including those related to procedures;processes;system and service parameters) logged;assessed and authorized prior to implementation and reviewed against planned outcomes following implementation (including impact from an information security perspective)?" was answered incorrectly. Question: NIST-R0040-CM-04.01 Answer: Partially Implemented Question Risk Score: 0.5 | Awaiting Review | Configuration Management | | Remediate Risk |
| FND-318 | The question: "Do you have processes in place to monitor and control changes to the baseline configuration settings of information systems in accordance with organizational policies and procedures?" was answered incorrectly. Question: NIST-R0042-CM-06 Answer: Not Implemented Question Risk Score: 1 | Awaiting Review | Configuration Management | | Remediate Risk |
| FND-319 | The question: "Do you have processes in place to monitor software usage in accordance | Awaiting Review | Configuration Management | | Accept Risk |

- Once you have addressed all the findings, click **Edit** on the questionnaire, and scroll down to the Findings Approval Workflow section to submit the questionnaire for review.

The Findings Approval Workflow section displays.

| ▼ Findings Approval Workflow | | | | | |
|-------------------------------------|---|-----------------|-------------------------------|----------------------|----------------|
| Assessor Finding Submission Status: | <input type="radio"/> In Process <input type="radio"/> Submitted | | Finding Submit Date: | <input type="text"/> | |
| Reviewer Finding Approval Status: | <input type="radio"/> Awaiting Review <input type="radio"/> Approved <input type="radio"/> Rejected <input type="radio"/> N/A | | Reviewer Finding Review Date: | <input type="text"/> | |
| Finding Reviewer Notes: | <input type="text"/> | | | | |
| Quantitative Summary | | | | | |
| Inherent Risk: | Low | | Residual Risk: | Low | |
| Inherent Risk Score: | 94.19 | | Residual Risk Score: | 97.67 | |
| ▼ Findings | | | | | |
| Finding ID | Finding | Status | Category | Criticality | Response |
| FND-317 | The question: "Are changes to information systems (including those related to procedures;processes;system | Awaiting Review | Configuration Management | | Remediate Risk |

9. Choose the **Submitted** radio button in the **Assessor Finding Submission Status:** section.

| Findings Approval Workflow | | | |
|-------------------------------------|---|-------------------------------|--|
| Assessor Finding Submission Status: | <input type="radio"/> In Process <input checked="" type="radio"/> Submitted | Finding Submit Date: | <input type="text"/>  |
| Reviewer Finding Approval Status: | <input type="radio"/> Awaiting Review <input type="radio"/> Approved <input type="radio"/> Rejected <input type="radio"/> N/A | Reviewer Finding Review Date: | <input type="text"/>  |
| Finding Reviewer Notes: | <div style="border: 1px solid #ccc; height: 40px;"></div> | | |

*The **Finding Submit Date** field is automatically populated with today's date.*

10. Click **Save and Close**.

The Reviewer receives an email stating that the findings actions are ready for review and approval.

Note: The Residual Risk Score is now higher than the Inherent Risk Score, indicating that by remediating some risks, your overall risk position is lowered.

Activity 9: Approve or Reject Finding Submission

Reviewer Activity (If Assigned)

You will receive an email from <DIR GRC noreply@Archerirm.us> notifying you that findings have been reviewed and that you must review and approve the action being taken on the findings.

1. Click the questionnaire number link in the email to review this response.



You will be directed to a login page.

2. Log in to your SPECTRIM account. See 4.0 Logging into SPECTRIM on page 7 for instructions on how to log in.

The completed assessment questionnaire opens, displaying the findings that must be reviewed and approved.

Activity 10: Forward Completed RAU to ISO for Approval

Risk Assessment Coordinator Activity

When all questionnaires are completed for an RAU, the RAC will see the combined risk score on the main RAU screen. This is the combined inherent and residual risk score for all the questionnaires for this RAU. This displays below the questionnaires on the screen.

| Questionnaire ID | Application | Launch Date | Assessor | Progress % | Overall Assessment Status | Inherent Risk | Residual Risk |
|------------------|---------------------|-------------|--------------|------------|---------------------------|---------------|---------------|
| 209121 | Bat tracking system | 6/5/2015 | Smith, Sally | 100.00 % | Findings Approved | Low | Low |

| Risk | | | |
|----------------------|--|----------------------|--|
| Inherent Risk: | <div style="width: 94.77%;"><div style="width: 94.77%;"></div></div> | Residual Risk: | <div style="width: 97.27%;"><div style="width: 97.27%;"></div></div> |
| Inherent Risk Score: | 94.77 | Residual Risk Score: | 97.27 |

Risk Assessment Coordinator ISO/Business Owner Approval Organization Head Approval

| Risk Assessment Coordinator | |
|-------------------------------------|----------------------|
| Risk Assessment Coordinator Status: | Assessments Launched |
| Risk Coordinator Notes: | |

| Approval Document Attachments | | | |
|-------------------------------|------|------|-------------|
| Name | Size | Type | Upload Date |
| No Records Found | | | |

SPECTRIM calculates Inherent and Residual Risk Scores. The RAC must now review the responses and forward them to the ISO for approval.

Risk Assessable Unit (Risk Project): 2016 Risk Assessment

New Copy Save Apply Edit Delete

| General Information | |
|---------------------|---------------------------|
| Project Name: | 2016 Risk Assessment Form |

1. Click **Edit** and scroll to the bottom of the screen.
 - *Risk Assessment Coordinator Status*: Select *Submit for Approval* from the dropdown box.
 - *Risk Coordinator Notes*: Include any notes that would be useful to the ISO in approving this RAU.
2. Click **Save**.

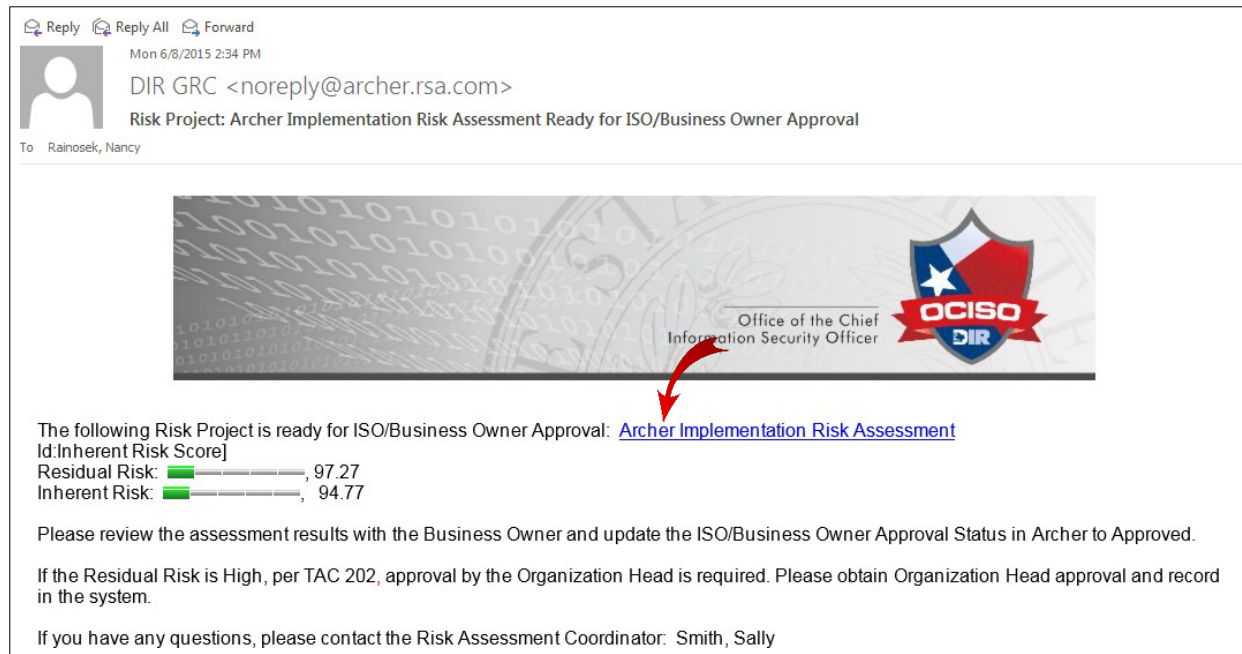
10.0 Approving the Risk Assessable Unit

Activity 11: Approve or Reject the RAU

Information Security Officer Activity

The ISO will receive an email requesting to review and approve or reject the RAU.

1. Click the link in the email to review this response.





The screenshot shows an email interface with the following content:

- Buttons: Reply, Reply All, Forward
- Date: Mon 6/8/2015 2:34 PM
- From: DIR GRC <noreply@archer.rsa.com>
- Subject: Risk Project: Archer Implementation Risk Assessment Ready for ISO/Business Owner Approval
- To: Rainosek, Nancy

The email body features a header banner with a background of binary code and a seal. The banner includes the text "Office of the Chief Information Security Officer" and the "OCISO DIR" logo. A red arrow points from the logo area to the text below.

The following Risk Project is ready for ISO/Business Owner Approval: [Archer Implementation Risk Assessment](#)
Id:Inherent Risk Score]

| | | |
|----------------|---|-------|
| Residual Risk: |  | 97.27 |
| Inherent Risk: |  | 94.77 |

Please review the assessment results with the Business Owner and update the ISO/Business Owner Approval Status in Archer to Approved.

If the Residual Risk is High, per TAC 202, approval by the Organization Head is required. Please obtain Organization Head approval and record in the system.

If you have any questions, please contact the Risk Assessment Coordinator: Smith, Sally

You are directed to a login page.

2. Log in to your SPECTRIM account. See 4.0 Logging into SPECTRIM on page 7 for instructions on how to log in.

The RAU screen displays.

3. Click across the tabs to see the various questionnaires that make up the overall RAU. To approve or reject the overall RAU in conjunction with the Business Owner, click the **ISO/Business Owner Approval** tab.

The screenshot displays a web interface for risk assessment. At the top, there is a 'Risk' section with two progress bars: 'Inherent Risk' and 'Residual Risk'. Below these are the scores: 'Inherent Risk Score: 94.77' and 'Residual Risk Score: 97.27'. A red arrow points from the 'Residual Risk' progress bar to the 'ISO/Information Owner Approval' tab. The interface has three tabs: 'Risk Assessment Coordinator', 'ISO/Information Owner Approval' (which is selected), and 'Organization Head Approval'. The 'ISO/Information Owner Approval' section contains a dropdown menu for 'ISO/Information Owner Approval Status' (set to 'Awaiting Review'), a date field for 'ISO/Information Owner Approval/Rejection Date' (set to '6/8/2015'), and a large text area for 'ISO/Information Owner Approval Notes'. At the bottom, there is an 'Approval Document Attachments' section with a table header: 'Name', 'Size', 'Type', 'Upload Date', and an 'Add New' link. The table currently shows 'No Records Found'.

The ISO/Information Owner Approval section displays.

4. In the **ISO/Business Owner Approval Status** dropdown box, choose from three options:
 - a. **Reject the RAU** and send it back through the process.
 - b. **Approve the RAU.**
 - c. **Approve the RAU and send it to the Organization Head** for approval if residual risk is high.

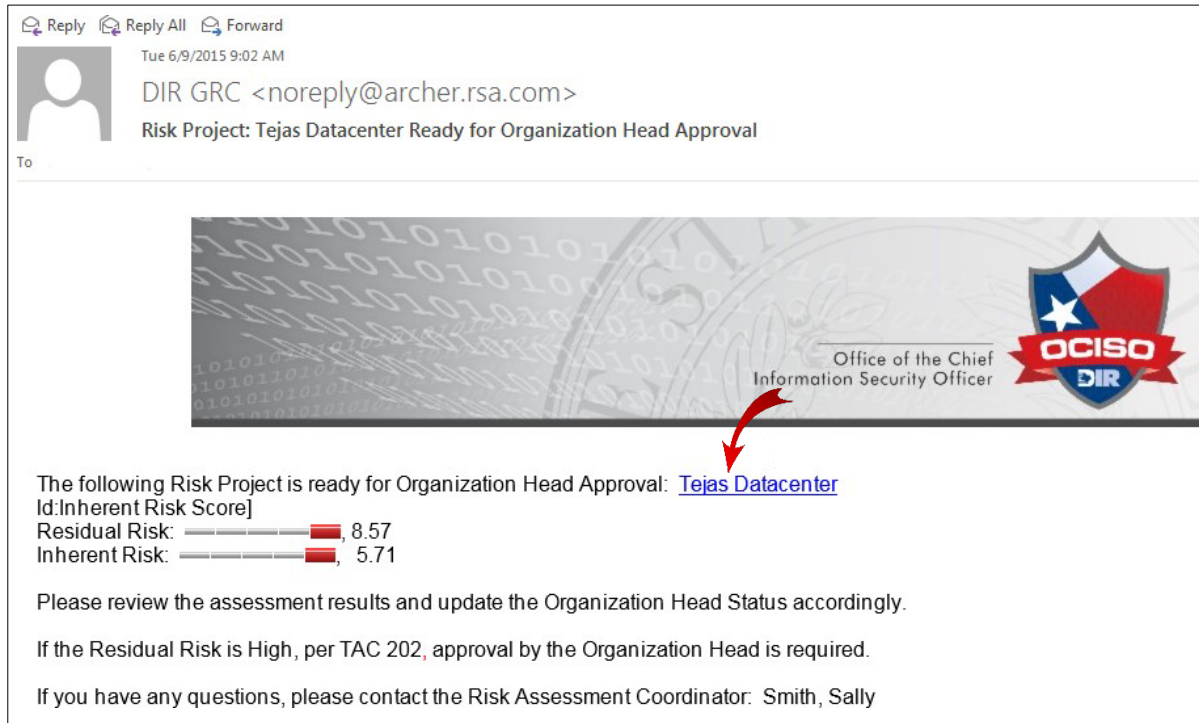
Note: If residual risk is high, arrange to gain approval from the organization head. See Activity 12: Approve or Reject the RAU on page 68.

Activity 12: Approve or Reject the RAU

Organization Head Activity

If residual risk is high, the person designated in the Organization Head field will receive an email to review and approve or reject the RAU.

1. Click the link in the email to review this response.



You are directed to a login page.

2. Log in to your SPECTRIM account. See 4.0 Logging into SPECTRIM on page 7 for instructions on how to log in.

The RAU screen displays.

3. Click across the tabs to see the various questionnaires that make up the overall RAU. To approve or reject the overall RAU, click the **Organization Head Approval** tab.

The screenshot shows a web interface for Risk Assessment. At the top, there are two tabs: 'Inherent Risk' and 'Residual Risk'. Below these, there are two score boxes: 'Inherent Risk Score: 5.71' and 'Residual Risk Score: 8.57'. A red arrow points from the 'Residual Risk' score to the 'Organization Head Approval' tab, which is currently selected. The 'Organization Head Approval' section contains a dropdown menu for 'Organization Head Approval Status' (set to 'N/A'), a date field for 'Organization Head Approval/Rejection Date', and a large text area for 'Organization Head Approval Notes'. Below this is a table titled 'Approval Document Attachments' with columns for 'Name', 'Size', 'Type', and 'Upload Date'. The table currently shows 'No Records Found' and has an 'Add New' button on the right.

The **Organization Head Approval** section displays.

4. In the **Organization Head Approval Status** dropdown box, choose from two options:
 - a. **Reject the RAU** and send it back through the process.
 - b. **Approve the RAU.**
5. If the approval was gained during a meeting and someone else is acting as the organization head, you can attach an email or other documentation indicating organization head approval. In the **Approval Document Attachments** section, click **Add New** and select the document to upload.

This is a close-up of the 'Approval Document Attachments' table. The table has a header with columns: 'Name', 'Size', 'Type', and 'Upload Date'. Below the header, it says 'No Records Found'. In the top right corner of the table, there is a button labeled 'Add New'. A red arrow points to this button.