ISO/IRM/Security Office:

- Moved current I-View’s on the page
- Created a New I-View that includes RAU’s by Risk Coordinator
General User: Assessor or Reviewer

- They will no longer have access to the RAU (Risk Project) Information Workspace (shown above). It will take the user to the Risk Assessments Workspace shown below.
- Moved I-View for better visibility: My Assessments Needing Action: This is to allow users to quickly see what they are assigned to and what Status it is in.
Left Navigation Menu Changes:

- Changed the order of how items are displayed
- Added Divisions into the hierarchy to accommodate organizations wanting to perform risk assessments at a deeper level. Note: If your organization is wanting to do this, please contact GRC@dir.texas.gov for more assistance. Even if you do not have any divisions associated to your organizations, you will see the Divisions tab. If you do have Divisions listed, a general user will have Read Rights to the Divisions. (This will have the look and feel like Organizations)
**RAU Changes**

- Adding a new RAU: You will be required to fill out required fields BEFORE scoping can begin. There have been many situations where the RAU was not saved before the assessments so the linkage between the two was lost. You will see the following message until you SAVE the record:

```
Please Note: You will not be able to Scope the RAU (i.e Applications, Networks, or Locations and related assessments) until your RAU has been created. Please fill out the required fields and click “Apply” and then you will see the appropriate content to begin scoping.
```

See Screenshot below: The user cannot see any related content yet.
After the “Apply” : The expected content shows

### RAU Field Changes

- **Division**: Again this is optional and has been designed for those wanting to perform risk assessments at a lower level. The help text describes it in detail.

- **Risk Assessment Coordinator Field**: Now required. In the past it did populate with the record creator (This will still be the case) however, it is now a required field that must be populated.

- **ISO**: The ISO field is not required and can only be filled out by the security office. This has been changed to accommodate other changes in SPECTRIM. If the ISO field is left blank, SPECTRIM will populate it with the Designated ISO (At the Organization Level). This will be evaluated on a daily basis.
**Application Specific Changes**

- Addition of two fields: (Note they are not required and include detailed help text of the purpose)
  - # of Units
  - Asset Value

<table>
<thead>
<tr>
<th>Description:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td># of Units:</td>
<td></td>
</tr>
<tr>
<td>Asset Value:</td>
<td></td>
</tr>
</tbody>
</table>

**Application, Location, Network Changes:**

**Field Changes**

- Addition of Division Field: This will allow those using the division functionality to tie a specific application, location or network to a specific division: Please note: All users within an organization are able to view All Applications, Locations or Networks even if it is Division Specific.
- ID Field: The ID field has changed to accommodate a Division. If a Division is present within the record, it will now combine the following: Name + Organization Number + Division Number.
  - Please see examples below:
    - Organization Specific Application: Employee Payroll System - 0
    - Division Specific Application: Employee Payroll System - 0 - 0
- The Inherent Risk as well as the Residual Risk has been added to the Assessment Information. This shows the rating scale instead of just the score.
- Added the Findings reference: This will show you all findings related to the specific Application, Location or Network
- Added field called: Secondary Organizations. This is to accommodate an application that ties to multiple organizations. This would be beneficial to those who are associated to multiple organizations.

**Updated Displays For Specific Users:**

- General User: We have removed the ability for a General User to see the Risk Score Section as well as the Findings section within the Application, Location or Network. If a user is associated to the specific assessment that was performed against a particular Application, Location or Network, they will be able to view it at that level
- Security Office, ISO, IRM: Will be able to see the Score Section as well as the Findings Section.
Updated Displays For Specific Users:

- General User: We have removed the ability for a General User to see the Risk Scores for the Organizational Security Assessment that has been performed.
- Security Office, ISO, IRM: Will be able to see the Risk Scores for the Organizational Security Assessment.
Risk Assessments:

Notifications:

- We have changed the look and feel of the notifications to give a cleaner look. Please see example below.

![Example Notification Image]

*gen user, michelle*

A risk assessment questionnaire has been launched and is ready for your completion. Once you are finished, submit for review and the appropriate reviewer will be notified. Please see details below:

**Questionnaire:** 239344  
**Application:** Test 5/4-0.  
**Due Date:**

If you have questions or need assistance, please contact the **Risk Assessment Coordinator**:

![OCISO Logo]

- **Additional Notifications: (TBD Date):** We are working to create a notification that goes to the Assessor with the Risk Assessment Coordinator of the Assessment when the Overall Status of the Assessment Record is Findings In Process with Assessor. This will be a digest email once a week. More details to come. We are seeing in production that there are several findings that have not been acted upon. This is just a friendly reminder that action is required.
Risk Assessment Field Changes:

- Security Office Field: The user that creates the record (Risk Assessment Coordinator) will be populated within the Security office field. We have found that most of the time this is the same user. However, you can change this if needed.