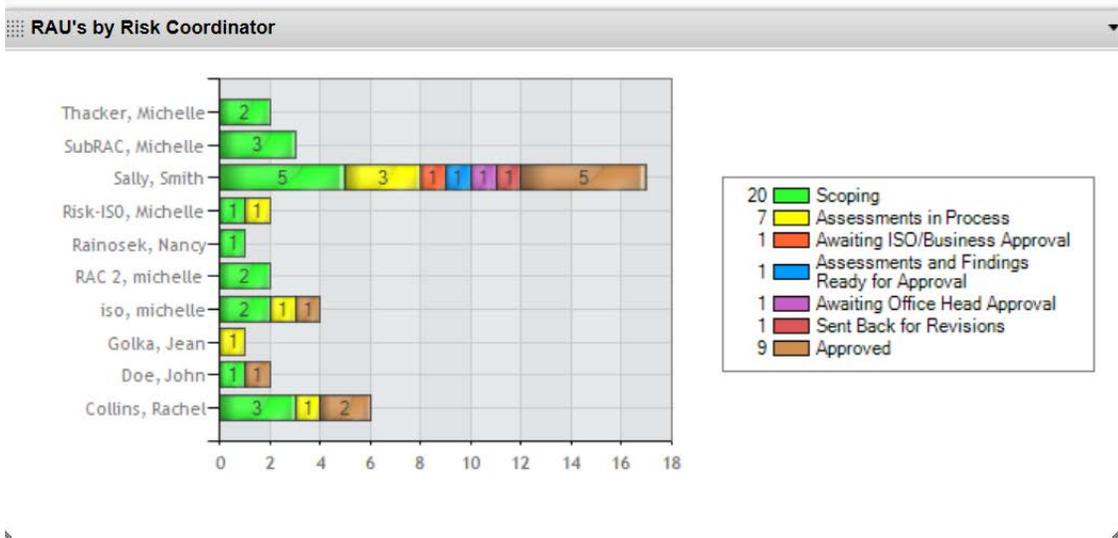
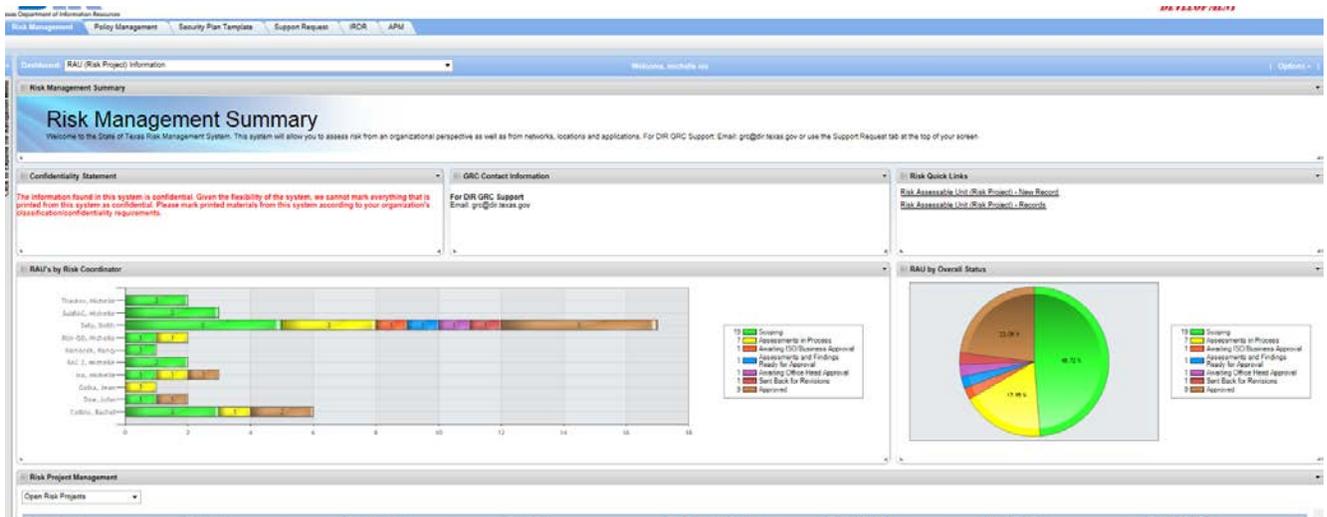


Risk Updates – March 2016

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.

Risk Management Summary

Welcome, michale.grover

My Assessments Needing Action

Questionnaire ID	Application	Progress %	Overall Assessment Status	Due Date	Assessor	Reviewer	Security Office
239173	Jean Test ISO - Application #1-0-	100.00 %	Awaiting Review by Reviewer	2/4/2010	Risk-General, Michale	jan.user.michale	jan.michale
239220	test-0-	100.00 %	Awaiting Review by Security Office		jan.user.michale	jan.michale	jan.michale
239222	Test Application 0-	100.00 %	Awaiting Review by Reviewer	2/17/2010	jan.user.michale	Risk-General, Michale	jan.michale
239223	Test Application 0-	100.00 %	Rejected by Reviewer		jan.user.michale	Risk-General, Michale	jan.michale
239224	Test Application 0-	100.00 %	Rejected by Security Office		jan.user.michale	Risk-General, Michale	jan.michale
239229	Test Application 0-	0.00 %	In Process by Assessor		jan.user.michale	Risk-General, Michale	jan.michale



My Assessments Needing Action

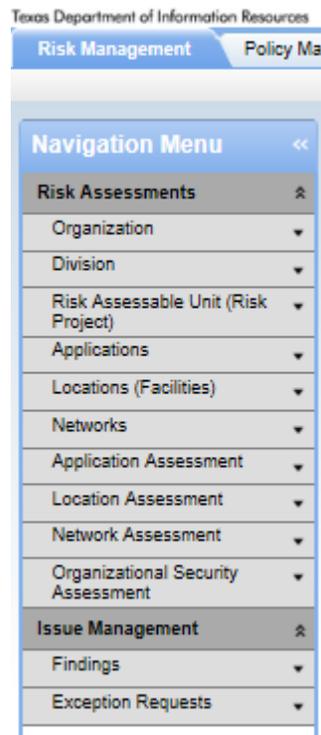
My Application Assessments Needing Action ▼

Questionnaire ID ▲	Application	Progress %	Overall Assessment Status
<u>239175</u>	<u>Jean Test ISO - Application #1-0-</u>	100.00 %	Awaiting Review by Reviewer
<u>239220</u>	<u>test-0-</u>	100.00 %	Awaiting Review by Security Office
<u>239222</u>	<u>Test Application 0-</u>	100.00 %	Awaiting Review by Reviewer
<u>239223</u>	<u>Test Application 0-</u>	100.00 %	Rejected by Reviewer
<u>239224</u>	<u>Test Application 0-</u>	100.00 %	Rejected by Security Office

A

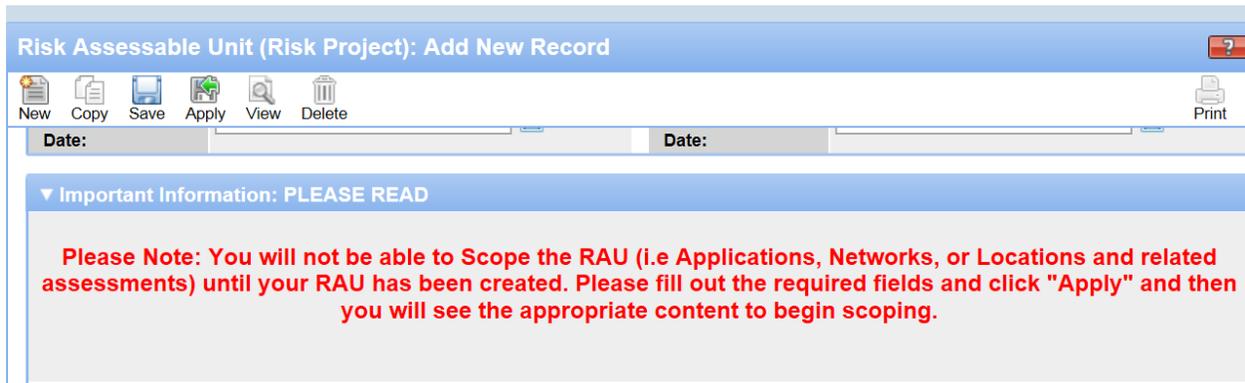
Left Navigation Menu Changes:

- 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)

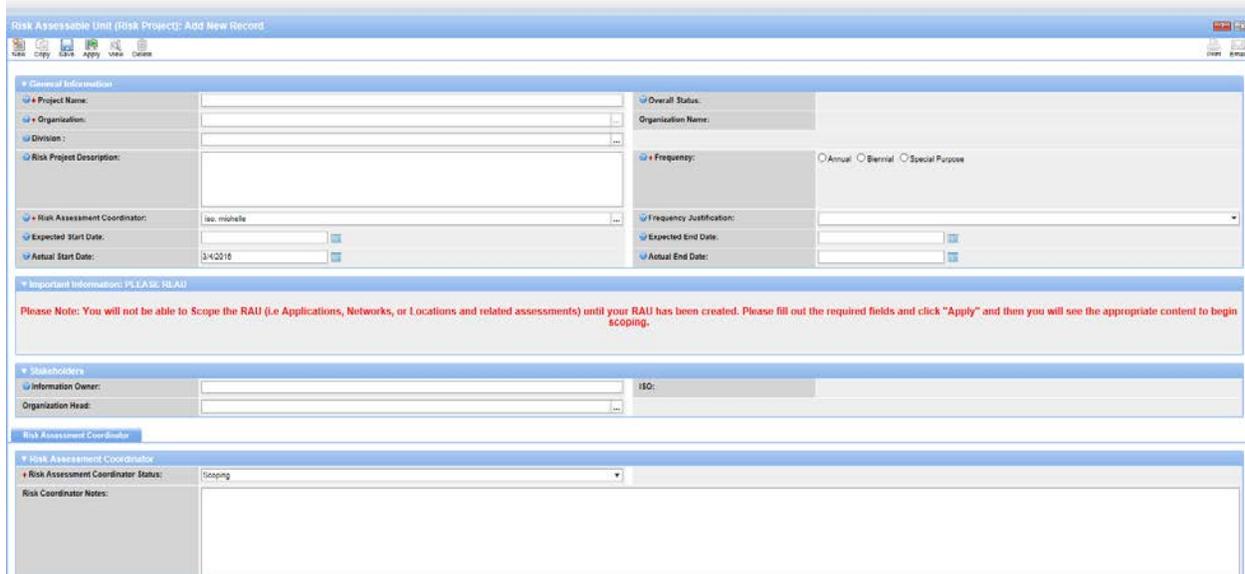


RAU Changes

- 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



See Screenshot below: The user cannot see any related content yet



After the “Apply” : The expected content shows

▼ Assessment Scoping

Please select the appropriate assessment components included in the scope of the assessment, including: applications, networks and locations. 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 the NIST questionnaire type selected for each component.

As you add new assessments, please identify the Assessor, the Reviewer (if needed) and Security Office personnell responsible for reviewing the asse

Recommended Security Category: Not Rated

Applications Locations Networks Organization Security Program Assessment

▼ Applications

ID	Information System Name	Organization Name
No Records Found		

▼ Application Assessment(s)

Questionnaire ID	Application	Launch Date	Assessor	Revi
No Records Found				

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.

▼ General Information

Project Name: Test Demo
Updated by iso, michelle on 3/4/2016 8:48:18 AM

Organization: [input field]

Division : [input field]

- 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

Description:		
# of Units:		Asset Value:

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.

No Records Found

Application Security Assessment(s)						
Last Approved Assessment Date:	2/26/2016					
Inherent Risk:			Residual Risk:			
Inherent Risk Score:	97.62		Residual Risk Score:		97.62	
Application Assessment(s)						
Questionnaire ID	Assessor	Launch Date	Progress %	Overall Assessment Status	Inherent Risk Score	Inherent Risk
238806	gen.user_michelle	2/26/2016	100.00 %	Finding(s) In Process by Assessor	97.62	Low
225733	Risk-General_Michelle	4/17/2015	100.00 %	Findings Approved	99.18	Low
239214	gen.user_michelle		100.00 %	Findings Approved	97.62	Low
225762			0.00 %	In Process by Assessor		Not Rated

Organization

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

Organization: 0

New Copy Save Apply Edit Delete

Record 1 of 1

First Published: 11/10/2014 1:58 PM Last Updated: 3/1/2016 4:30 PM

General Information Other Details **Risk Assessment Information** Assessment Training Completion Information

▼ Risk Assessment

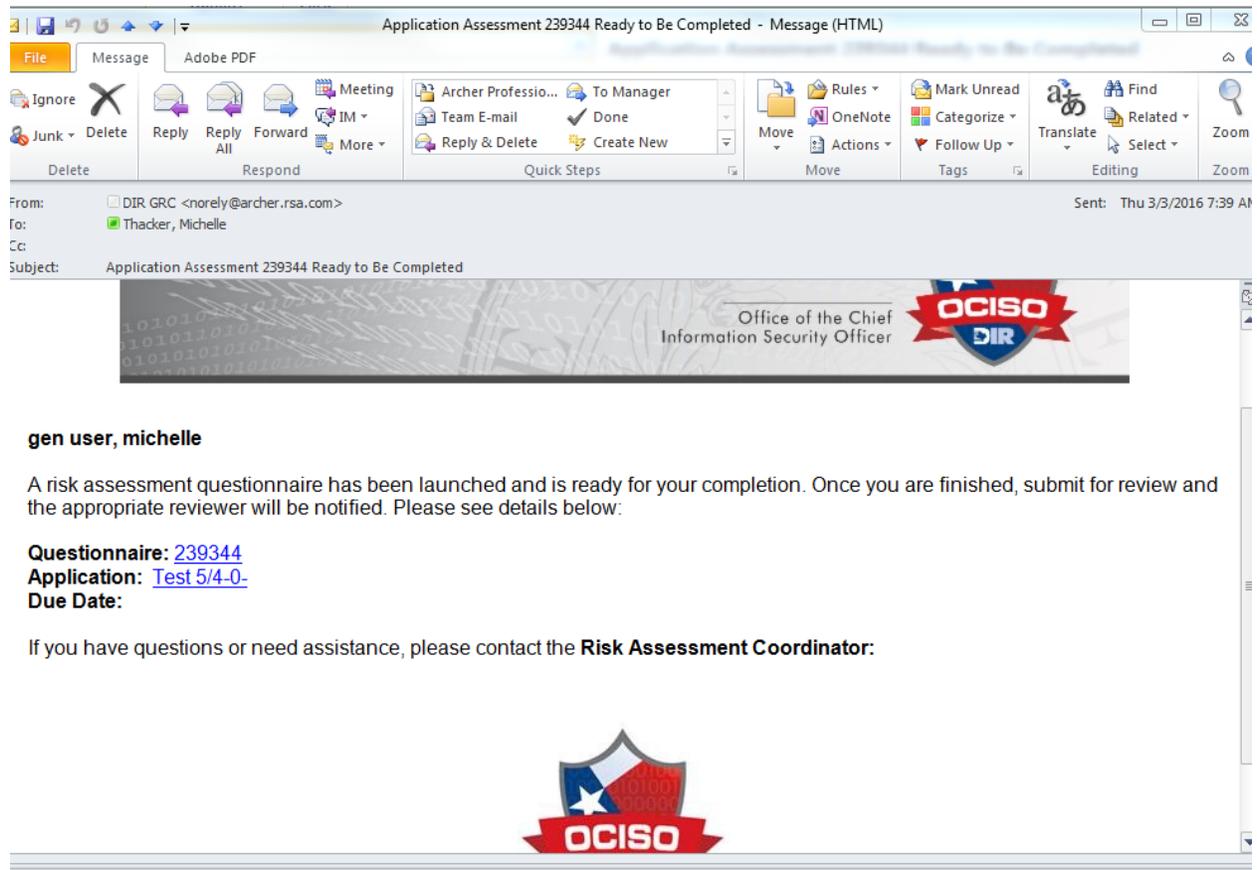
NIST Questionnaire Type:	NIST Low	Last Organizational Security Assessment:	
Residual Risk:		Residual Risk Score:	100.00
Inherent Risk:		Inherent Risk Score:	100.00

► 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.



The screenshot shows an Outlook email window titled "Application Assessment 239344 Ready to Be Completed - Message (HTML)". The email header includes the sender "DIR GRC <norely@archer.rsa.com>" and the recipient "Thacker, Michelle". The subject is "Application Assessment 239344 Ready to Be Completed". The email body features a header for the "Office of the Chief Information Security Officer" (OCISO) with a logo. The main text of the email reads: "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:", and "If you have questions or need assistance, please contact the **Risk Assessment Coordinator**:". The OCISO logo is displayed at the bottom of the email content.

- **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.

Instructions

General Information			
Questionnaire ID:	239358	Overall Assessment Status:	In Process by Assessor
Network:	Test 5/4-0-	Progress %:	0.00 %
Organization Name:	State Agency for Archer	Due Date:	
Risk Assessment Coordinator:	iso_michelle	Assessor:	gen.user.michelle
Launch Assessment:		Reviewer:	
Launch Date:		Security Office:	iso_michelle
History Log:	View History Log		