

## TABLE OF CONTENTS

<b>1 Purpose .....</b>	Error! Bookmark not defined.
ASM Process.....	3
Automation of the Program Protection Plan.....	5
<b>2 General ASM Tool Navigation .....</b>	7
Accessing ASM via SIPRNET .....	7
Associate Your SIPR Token:.....	7
ASM Main Menu (Main Home Page) .....	8
Manage Assessments Screen.....	9
Create a New Assessment Screen.....	9
Assessment Name.....	11
ASM Naming Convention.....	11
Node.....	11
Assessment Objective .....	11
Due Date .....	12
Reviewing/Editing a Previously Created Assessment .....	13
<b>3 Assessment Home Page – Main Menu.....</b>	14
Assessment Home Page - Administration.....	15
Data Collection Page .....	16
Profile Screens .....	17
Profile Organization – Describe the Organization .....	17
Profile Page 1 Profile Page 1 – Describe the Operating Environment Drop Down menus.....	19
Profile Page 2 - Scope the Assessment- Questions.....	23
Profile Page 2, Describe the operating Environment, continued – Technology Areas - Asset Groups.....	25
Asset Page .....	26
Asset Page, Additional Functionality.....	27
Adding a Missing Asset .....	29
Using Excel to Complete the Asset Page (Export to Excel) .....	30
Upload the Assets (upload Responses).....	31
Threat Page .....	32
Threat Option Buttons .....	33

Threat Changes - ***Requires detailed reason*** .....	33
Countermeasures Page .....	35
Countermeasure Option Buttons.....	36
Export to Excel Functionality .....	37
Upload Responses.....	37
Finish and Lock Assessment.....	40
Basic Analysis, Mitigation and Submission Page.....	41
Risk Tab .....	41
Compliance Tab.....	47
<b>4 Program Protection Plan .....</b>	<b>49</b>
Create a PPP Outside of an Assessment .....	49
Update the PPP .....	50
When completing the Program Protection Plan:.....	53
Other PPP Functions .....	53
<b>5 Reports.....</b>	<b>Error! Bookmark not defined.</b>
Single Assessment Reports .....	54
Multiple Assessment Reports .....	54
Recommended Reports for ASM .....	54
Executive Summary Report.....	54
Dashboard Report.....	55
<b>6 Advanced Analysis .....</b>	<b>56</b>
Advanced Analysis – Reports and Other Features.....	58
Advanced Analysis – Sample Reports .....	60
<b>8 View References and Materials .....</b>	<b>64</b>
<b>9 ASM Dedicated Help Page .....</b>	<b>65</b>
<b>10 ASM Demo Account .....</b>	<b>66</b>
Purpose .....	66
Access.....	66
Getting a login for the demo account.....	67

# CHAPTER 2 OVERVIEW OF THE ASM TOOL

## 1 Purpose

The purpose of this chapter is to provide the basic navigation and functionality of the ASM tool. It also defines the drop-down menus in each of the pages.

### Things to keep in mind when using the ASM Tool:

- **Learn the basics first** - ASM has many functions. Learning them all at once can be overwhelming. Work from the job aids then expand your knowledge as you progress.
- **Use the Demo account** – The demo account (unclassified) has the same functionality as the SIPR account but has notional data. It is a great way to familiarize yourself with the tool without worry of affecting real data.
- **Ask for help** - A quick phone call or email can save hours of time trying to remember how to do a task. Reach out to the ERPM Help Desk whenever assistance is needed.
- **Provide feedback** - Keep track of your feedback so the tool can continue to improve.
- **Trust the tool** – Many hours of work went into the background data to determine the correct countermeasures questions based on 29 different references. Threat and asset values were also researched and based on DSCA recommendations. All factors contribute to the risk calculation.
- **Trust the process** - The tool takes you through a step-by-step process. Follow the steps and answer the questions on each page.
  - All work is saved as you go along so no need to worry about lost work.
  - If you need additional input from other groups, every page has an export function enabling you to export the data for discussion.

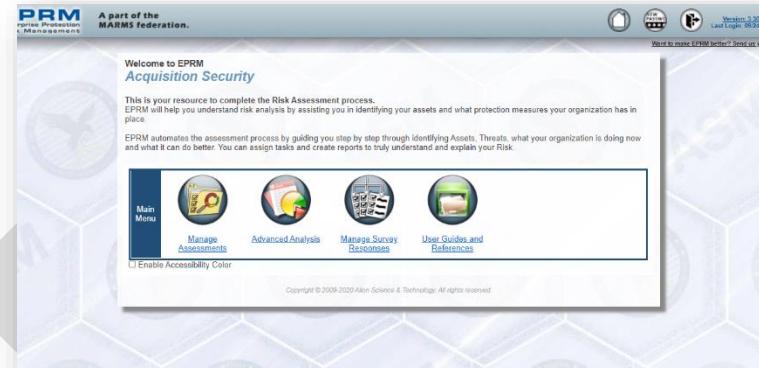


Figure 1: ASM 1

## ASM Process

The ASM process was developed to automate some of the tasks already being done in the acquisition process. The diagram below shows the steps in the ASM process. Creating the Baseline assessment is most time consuming. All other assessments except the Baseline are done from copy so the process is very efficient. The following page shows the step by step process:

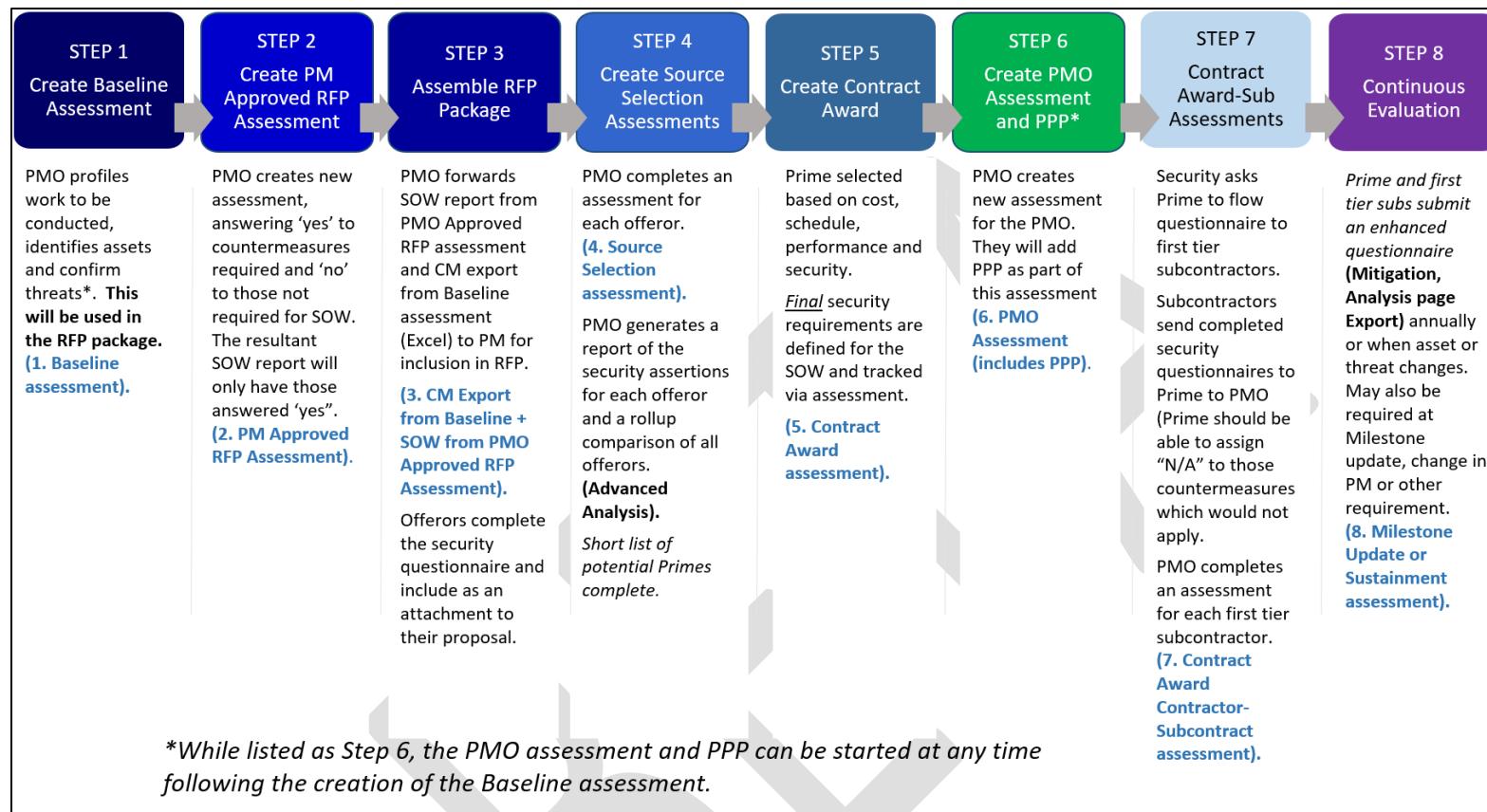


Figure 2: ASM Process

## Automation of the Program Protection Plan

The ASM process includes automated tracking of the Program Protection Plan (PPP) as part of the assessment process. When Program Management Offices (PMOs) conduct their own assessment, they can click a link to create the Program Protection Plan. While this shows as Step 6 of the process, the PPP can be started at any time.

**PROGRAM INFORMATION**

4. Does the program have a Program Protection Plan?

-- 4.a. If you are a PMO, please complete a PPP.

**Program Protection Plan**

5. What ACAT level is this?

**Link to get to Program Protection Plan on Profile Page 1 of Assessment. Here you can create a new PPP or associate a PPP already started.**

Figure 3: PPP Link

The Program Protection plan consists of three weighted questions from the PMO assessment and 21 compliance questions. Questions are answered “Yes”, “No” or scheduled. All questions have space for remarks and some questions require additional information.

[Home](#) > [Manage Surveys Home](#) > [3205 PPP New Created directly](#) > [1 - Data Collection](#) > Page 1

**Questions**  
Please answer the following questions.

**Program Protection Plan (PPP)**

This question is “Yes”, “No” or “Scheduled” with further information required.

1. Has a PPP been developed and approved for ALL programs beginning at MS A and every subsequent Milestone Decision including Full-Rate Production, and approved by the MDA?

PPP Date Approved:   
PPP Date Due:

PPP Required Documentation submitted?\*

PPP Remarks:

This question is “Yes”, “No” or “Scheduled” without further information required.

1.a. Have system modifications or upgrades been made?  with provisions for annexes to cover future modifications. (Note: The annex is effectively a “stand alone” PPP for the modification/upgrade effort.)

System Modification Remarks:

2. Did the PM collaborate with the USAF AT Service Lead for Anti-Tamper Planning? (Note: SAF/AQL is the Air Force AT Service Lead)

AT Collaboration Remarks:

Figure 4: PPP Questions

Once created, the plan will show on the assessment page and be included in reports.

The screenshot shows a portion of an assessment form. At the top left, there is a dropdown menu labeled "have a Program Protection Plan?" with a red question mark icon. Below it, a section asks "If you are a PMO, please complete a PPP." A table row is highlighted with a red box, showing "Program Protection Plan" in the first column, "ID" in the second, and "Name" in the third, with the value "3205 PPP New Created directly". To the right of this table, a yellow callout box contains the text "The PPP associated with this assessment is shown here." At the bottom left, there are other form fields: "5. What ACAT level is this program?", a dropdown menu, and a text input field for "5.a. If other, please describe".

Figure 5: Associated PPP

As a program matures, the plan can be updated, including upload of files and documentation relative to the plan.

The screenshot shows a list of actions for a survey. From top to bottom, the buttons are: "Share this Survey" (description: Share this survey with other users), "Change Owner" (description: Give responsibility for this survey to another user), "Delete" (description: Permanently delete this survey), and "File/Image Upload" (description: Upload files or images). The "File/Image Upload" button is highlighted with a red box.

Figure 6: Easy upload of PPP files

**NOTE:** When completing the PPP, it is critical ALL to answer ALL questions then finish and lock the PPP. This ensures the data will be included in reports. The plan can be updated as often as needed.

## 2 General ASM Tool Navigation

### Accessing ASM via SIPRNET

To get to the tool:

Navigate via SIPRNET to: <https://eprm.csd.disa.smil.mil>

Enter your login information provided by the EPRM Help Desk.

#### Associate Your SIPR Token:

After you login the first time, you can associate your SIPR token with your email. This will allow you go directly to “Click Login” after inserting your CAC card.

To ensure you can log in with your token, please associate your SIPR token ID to your profile by following the steps below. Once you’ve completed the process, you will continue to login using a password until EPRM becomes SIPR token enabled.

User support will send an email out to everyone when usernames and passwords are no longer required. (Note: Per DoD Policy, accounts will still expire after 35 days of inactivity)

#### How to Register Your SIPRNET Token:

1. Click the Add SIPR Token ID to Your User Profile. (Fig. 1)
2. Enter your SIPR email address into the pop-up dialog box and click the Add Your SIPR Token ID to Your Profile button. (Fig. 2)
3. Immediately, check your SIPR inbox for the system generated email and confirm the registration.

**IMPORTANT:** As a security feature, completing step 2 above will lock the user’s account and generate a confirmation email to their SIPR inbox. Within the email users are asked to confirm their intention to register their token. Upon confirming the registration, the user’s account will be unlocked and ready for use. Failure to confirm the registration (step 3) will leave the user’s account in a locked state.



Figure 7: ASM Login screen on SIPRNe

## ASM Main Menu (Main Home Page)

The main menu shows four main icons used to navigate ASM. The table below each screen shot provides a brief description of each icon.

Icons located in the upper right section of the main menu enable users to log off system, get back to the home screen or change your password.

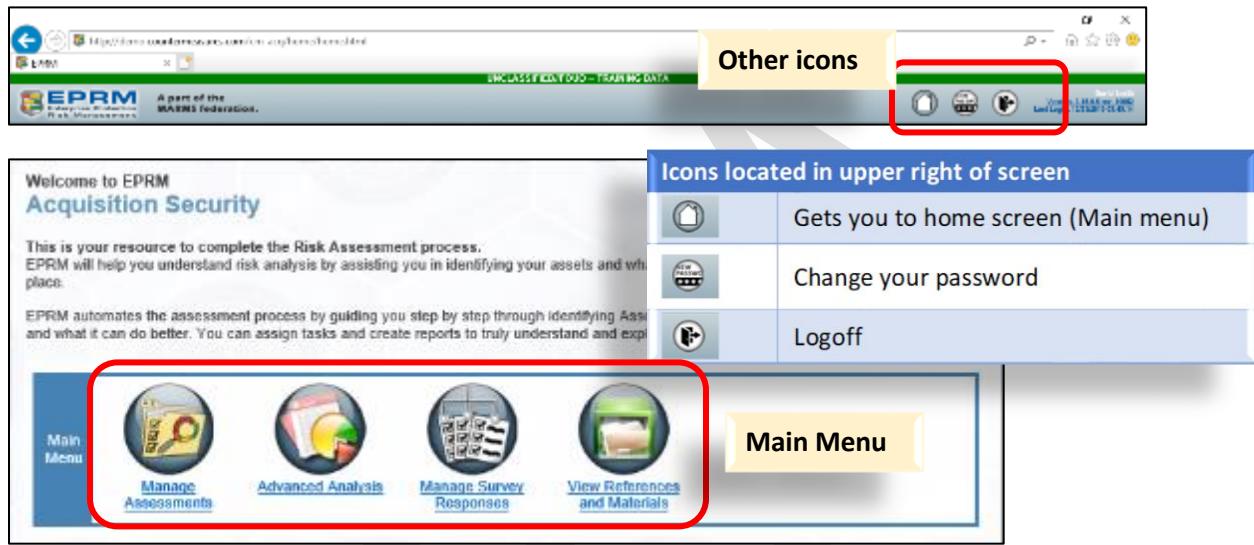


Figure 8: ASM main menu

If you are having trouble logging in, please contact the EPRM Help desk at [EPRMHELP@alionscience.com](mailto:EPRMHELP@alionscience.com)

Icon	Use to
<b>Manage Assessments</b>	Create assessments; review an already completed assessment, find an assessment
<b>Advanced Analysis</b>	Run multi assessment reports
<b>Manage Survey Responses</b>	Document and update PPP plan/survey
<b>View References and Materials</b>	Find resources and materials relative to EPRM (i.e., DoD documentation, checklists, job aides, etc.)

Figure 9: Main Menu Buttons Table

## Manage Assessments Screen

Clicking on **Manage Assessments** gets you to the Manage Assessments Home Page. This is where you can create a new assessment or view/modify existing assessments based on your privileges. This is where you can also see upcoming scheduled assessments.

The screenshot shows the 'Manage Assessments' screen with several key components:

- Main menu:** Located at the top right, it includes links for 'Main menu', 'Advanced Analysis', 'Manage Survey Responses', 'View References and Materials', and 'Main menu' (a self-link).
- Breadcrumbs menu:** Located below the main menu, it shows the path 'Home > Manage Assessments Home'. A callout box notes: "Breadcrumbs menu (tells you where you are and has hyperlinks to navigate)".
- Start button:** A large green button labeled 'START' with a white arrow pointing down, accompanied by the text 'Creates a New Assessment'.
- Starts a new assessment:** A callout box pointing to the start button.
- Filters:** A section titled 'Filters to help find a specific assessment' with a red arrow pointing to the filter input fields in the grid.
- Assessments Grid:** A table titled 'Started and Completed Assessments - To view an assessment, double-click on a row or select a row and click on open button at the bottom of the grid.' It lists columns: id, Assessment Name, Due Date, Status, Owner, Node, Created, and Objective(s). Data rows include:
 

id	Assessment Name	Due Date	Status	Owner	Node	Created	Objective(s)
4100	FIREBIRD15246-PRE-RFP-BASELINE		1 - Data Collection	Adrian Aspelin	AFLCMC > AFLCMC/EB PEO Weapons	09/25/2019	Acquisition Security
4102	FIREBIRD15246-PRE-RFP-BASELINE		1 - Data Collection				
4105	FIREBIRD15246-PRE-RFP-BASELINE		1 - Data Collection				
4106	FIREBIRD15246-PRE-RFP-BASELINE		1 - Data Collection				
4108	FIREBIRD15246-PRE-RFP-BASELINE		1 - Data Collection	John McCoy	AFLCMC > AFLCMC/EB PEO Weapons	09/25/2019	Acquisition Security
4109	TEST		1 - Data Collection	Cathy Sumeracki	AFLCMC > AFLCMC/EB PEO	09/25/2019	Acquisition Security
- Previously completed/started assessments:** A callout box pointing to the first few rows of the grid.
- Timeline:** A section titled 'Timeline (in months): 12' with a slider bar and the instruction: '\* Move slider left / right to change number of months for the Upcoming Assessments grid'.
- Timeline of scheduled assessments:** A callout box pointing to the timeline section.
- Upcoming Assessments:** A table titled 'Upcoming Assessments (next 12 months)' with columns: Start Assessment, Due Date, Last Completed, Frequency (months), and Duration (months). It shows one row of data.
- Upcoming (scheduled) assessments:** A callout box pointing to the 'Upcoming Assessments' table.

Figure 10: Manage assessments home page.

When in doubt, read the top portion of the screen.  
 Each screen explains purpose of the section and provides instructions.

## Create a New Assessment Screen

[Home](#) > Manage Assessments Home

This is where you may create a new assessment or view / modify existing assessments based on privileges or permissions unique to your User Profile. [\[More\]](#)

**START**  
Create a New Assessment

Home > Manage Assessments Home > New Assessment

**Let's get started with the Risk Assessment process.**  
We'll begin by creating a new assessment.

An \* denotes the field is required

Enter a short descriptive name for the assessment (see Assessment Name Examples below).

**Assessment Name\***

**Assessment Name (auto-populated)  
No need to enter this field.**

Assessment Name Examples  
 20180004-38th Air Base Wing-Wright Patterson AFB  
 1QTR19-DA-DLA (Format for DoD Counter Insider assessments, only)  
 FIREBIRD18240-Pre-RFP-Baseline (Format for Acquisition Security assessments, only)

Select the node you will be assessing from the hierarchy below. Use the (+) functionality to expand the tree until you find the correct node. You have the privilege to select any node in plain text. If you do not see the node available contact your administrator or the Help Desk to have it added.

**Node legend:**  
 Nodes in plain text are available to you in your assessment creation.  
 Nodes in gray strikethrough are expired.  
 Nodes on a dark background are not available to you.

**Search Nodes**

**Node (select one in plain text)\***

- (+) LISA Acquisition Security
  - (+) AF/CMC
  - (+) **AFNWC**
  - (+) ARL
  - (+) Air Force Space Command
  - (+) Other
  - (+) SAF/AQ
  - (+) SMC

**Node (organization). You may have to click on the “+” to expand to find your three-digit program.**

Select your assessment objective.

What kind of assessment will you be conducting?  Acquisition Security

**Objective** is Acquisition Security. Most users will only see Acquisition Security. However, if you have access to multiple objectives, you may see more.

Due Date  Clear Due Date

**Back** **Continue**

**Navigational buttons**

Figure 11: New Assessment Page

## Assessment Name

### **Name of the assessment (auto populated)- No need to enter**

ASM uses a standard auto naming convention so assessments can easily be identified. Over time, there will be many assessments across all programs. By using a standard naming convention outlined below, assessments can easily be filtered for and found in the future. The ASM keeps an electronic copy of every assessment.

The assessment name is *automatically populated* as you complete the assessment.

## ASM Naming Convention

The following syntax is used to name assessments:

Objective – Date started – Three letter Program – Program Name  
– Type of Assessment -CAGE code of Prime – Who provided Information – Name of Subcontractor (if applicable)

Here are some examples:

- ASM – 07/10/2020 - WWL - FIREBIRD - SOURCE SELECTION - 1651651615 – PRIME
- ASM – 07/30/2020 - WWL – FIREBIRD – CONTRACT AWARD – 1651651615 - SUBCONTRACTOR- ABC

If needed, you can change the name of the assessment. See Chapter on Additional Features instruction on renaming assessment.

## Node

### Select the Program Node

The ASM tool is organized by nodes which mirror the current Acquisition Security organization (in most cases). When getting access to the ASM, you were assigned a node relative to your role within the program. Users have access to the node(s) they were assigned and nodes below. Only the node(s) and the associated assessments and program protection plans to will show. In some cases, you may have to click on the plus sign (+) to expand the view to see all the nodes.

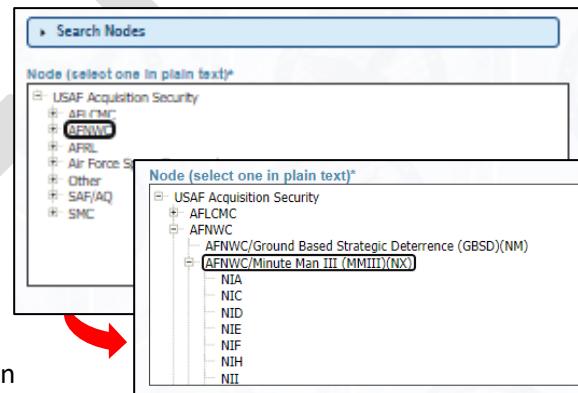


Figure 13: Node and expanded node

Figure 10: New Assessment page 1

## Assessment Objective

### Select Acquisition Security as the objective

Acquisition Security is the objective (or database).

For users with access to multiple objectives, you may see more than one option here.

What kind of assessment will you be conducting?

Figure 14: Type of Assessment (Objective)

## Due Date

### Disregard Due Date

Currently this date is not being used and is not required.

A screenshot showing a 'Due Date' input field with a calendar icon, a 'Clear Due Date' button, and a 'Save' button at the bottom right.

Figure 15: Due Date

### Continue/Back

These are navigational buttons.

A screenshot showing a 'Back' button and a 'Continue' button side-by-side.

Figure 16: Navigation buttons (Back and Continue)

Once assessment information is populated, click **Continue** to navigate to the new assessment page.

A screenshot of a web page titled 'Copy/Inherit Options'. It shows a 'Main Menu' with 'Manage Assessments', 'Advanced Analysis', 'Manage Survey Responses', and 'View References and Materials'. Below the menu, the URL is 'Home > Manage Assessments Home > 4503\_15446FIREBIRD-PRE\_RFP\_PMO ASSESSMENT > Copy/Inherit Options'. A section titled 'Would you like to:' contains instructions and two options: 'Copy from an existing assessment.' and 'Inherit from one or more previously created templates.'. The 'Copy from an existing assessment.' option is highlighted with a red box. To the right, a yellow box contains the text 'New assessment options'. At the bottom right is a 'Continue' button, also highlighted with a red box.

Figure 17: Assessment Creation Choices

**Templates** contain pre-populated values for assets and threats based on DSCA guidelines. The ASM CCB may periodically update templates. The ASM CCB is the only entity who has authority to update templates.

What	Description	Use When
<b>Copy from an existing assessment</b>	Creates an assessment based on a previously created assessment	Creating every other assessment except the BASELINE assessment
<b>Inherit from one or more previously created templates</b>	Creates an assessment based on a pre-populated value for assets and threats.	<b>Creating the BASELINE assessment</b>
<b>Continue</b>	Takes you to next screen	Ready to move forward

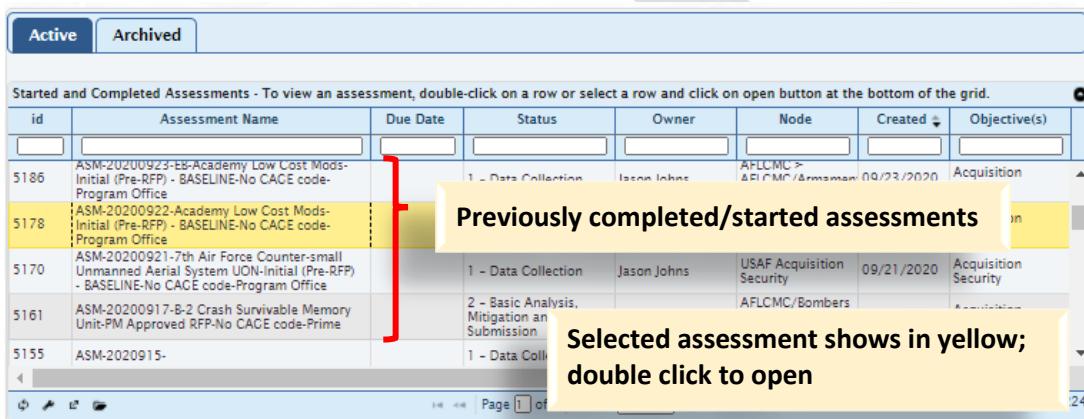
Figure 18: Creating a New Assessment Options

Figure 16: Assessment Creation Choices Table1

## Reviewing/Editing a Previously Created Assessment

ASM stores all assessments electronically. This includes completed assessments as well as any assessments started but not finished. These are located at the bottom half of the screen. Filter fields above each column enable you to filter to find a specific assessment. A yellow row indicates a selected assessment. Double click to open a yellow highlighted assessment.

The assessment list includes the assessments in a specific program. The user's position in the hierarchy shows assessments at the same level and below. AHQ will see all the assessments; PEOs will see the assessments across all their directorates; Program Managers see all assessments in their programs.

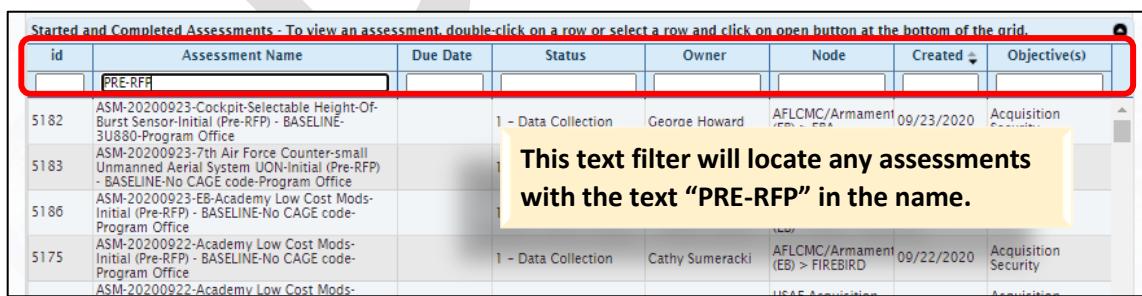


A screenshot of a web-based application interface titled 'Previously completed/started assessments'. The interface features a table with columns: id, Assessment Name, Due Date, Status, Owner, Node, Created, and Objective(s). The first row, which contains the text 'ASM-2020U923-EB-Academy Low Cost Mods-Initial (Pre-RFP) - BASELINE-No CACE code-Program Office', is highlighted with a yellow background. A red bracket on the left side of the table points to this yellow-highlighted row. A yellow callout box on the right side of the table contains the text 'Selected assessment shows in yellow; double click to open'.

Started and Completed Assessments - To view an assessment, double-click on a row or select a row and click on open button at the bottom of the grid.							
id	Assessment Name	Due Date	Status	Owner	Node	Created	Objective(s)
5186	ASM-2020U923-EB-Academy Low Cost Mods-Initial (Pre-RFP) - BASELINE-No CACE code-Program Office				AFLCMC > AFMC/Armament	09/23/2020	Acquisition
5178	ASM-20200922-Academy Low Cost Mods-Initial (Pre-RFP) - BASELINE-No CACE code-Program Office						
5170	ASM-20200921-7th Air Force Counter-small Unmanned Aerial System UON-Initial (Pre-RFP) - BASELINE-No CACE code-Program Office			1 - Data Collection	Jason Johns	USAF Acquisition Security	09/21/2020
5161	ASM-20200917-B-2 Crash Survivable Memory Unit-FM Approved RFP-No CACE code-Prime			2 - Basic Analysis, Mitigation and Submission		AFLCMC/Bombers	
5155	ASM-2020915-			1 - Data Col			

Figure 19: Manage Assessment – Previously Created Assessment List

**FILTER FIELDS:** When locating previously started/completed assessments, you can add text in any of the fields above the list to locate specific assessments. Use multiple filters to get more specific search parameters.



A screenshot of the 'Started and Completed Assessments' grid. A red box highlights the 'Assessment Name' column header. A yellow callout box on the right side of the grid contains the text 'This text filter will locate any assessments with the text "PRE-RFP" in the name.' The grid displays several rows of assessment data, with the first row being highlighted in yellow.

Started and Completed Assessments - To view an assessment, double-click on a row or select a row and click on open button at the bottom of the grid.							
id	Assessment Name	Due Date	Status	Owner	Node	Created	Objective(s)
	PRE-RFP						
5182	ASM-20200923-Cockpit>Selectable Height-Of-Burst Sensor-Initial (Pre-RFP) - BASELINE-3U880-Program Office			1 - Data Collection	George Howard	AFLCMC/Armament	09/23/2020
5183	ASM-20200923-7th Air Force Counter-small Unmanned Aerial System UON-Initial (Pre-RFP) - BASELINE-No CACE code-Program Office						
5186	ASM-20200923-EB-Academy Low Cost Mods-Initial (Pre-RFP) - BASELINE-No CACE code-Program Office						
5175	ASM-20200922-Academy Low Cost Mods-Initial (Pre-RFP) - BASELINE-No CACE code-Program Office			1 - Data Collection	Cathy Sumeracki	AFLCMC/Armament (EB) > FIREBIRD	09/22/2020
	ASM-20200922-Academy Low Cost Mods-						

Figure 20: Using filters to find assessments

### 3 Assessment Home Page – Main Menu

The assessment home page is where users can add information to an existing uncompleted assessment or utilize the Basic Analysis, Mitigation and Submission function to see risk and compliance for completed assessments.

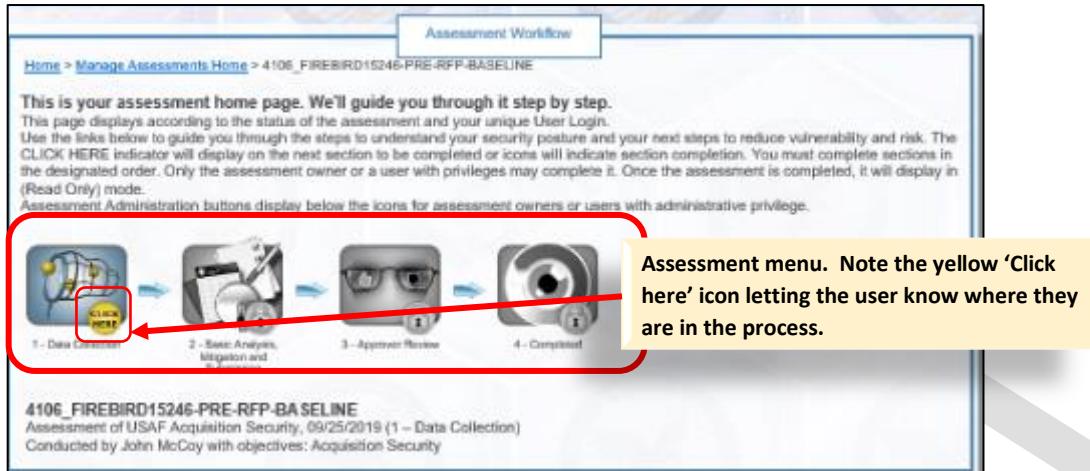


Figure 21: Assessment Home Page

Icon	Function
Data Collection	Starts the step by step process of creating an assessment
<i>NOTE: Other icons are gray and not available until assessment is complete.</i>	
Basic Analysis, Mitigation and Submission	An onscreen look at an individual assessment from risk and compliance perspective. This includes the detail of what is driving the risk score. This screen also enables an update on countermeasures with adjusted risk and compliance scores.
Approver Review	Enables a user to forward an assessment for approval. ( <i>Functionality not currently in use for ASM</i> ).
Completed	Complete a fully approved assessment. ( <i>Functionality not currently in use</i> ).

Figure 22: Table of Assessment Home Page Icons and Functions1

## Assessment Home Page - Administration

The Assessment Home page is the main menu for a specific assessment. The yellow circle on the icons lets you know where the assessment is in the process. In this example, the assessment is at data collection.

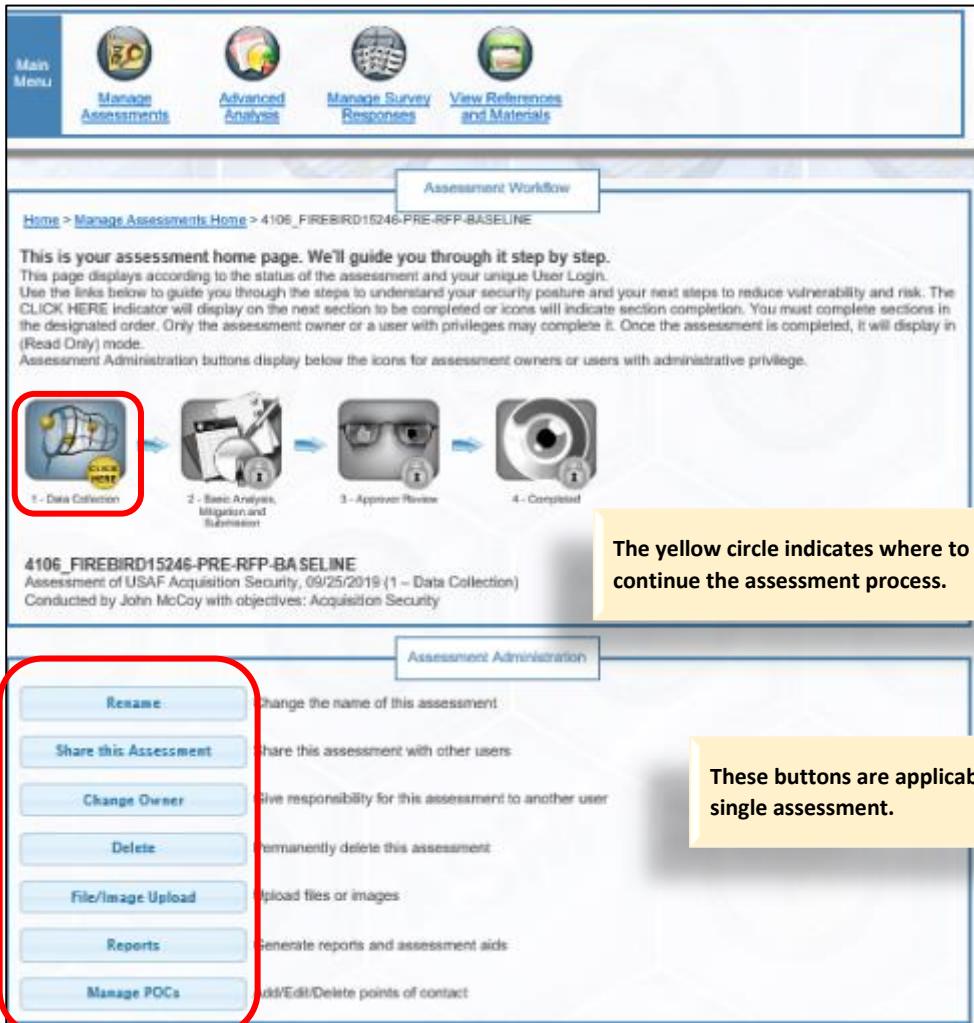


Figure 23: Assessment Home Page Administration Options

Button	Function
<b>Rename</b>	Rename an existing assessment if your naming convention is incorrect.
<b>Share this Assessment</b>	Share this assessment with a specific person within your hierarchy
<b>Change Owner</b>	PEOs Only: Change the owner of this assessment
<b>Delete</b>	PEOs Only: Assessment may only be deleted with Security Office approval
<b>File /Image upload</b>	Upload files and images relative to this assessment
<b>Reports</b>	View and print reports relative to this assessment
<b>Manage POCs</b>	Add key points of contract relative to this assessment

Figure 24: Table of Assessment Administration Options

## Data Collection Page

The data collection page takes the user step by step to complete an assessment. You can stop and pick up where you left off at any point in the assessment. ASM automatically tracks where you left off.

The first five steps present a series of questions users answer about the program. The final step locks the assessment. Circular badges at the lower right of each phase indicate the status of that step. Each subsequent step is locked until the previous step is completed. A check mark indicates a completed step.



Figure 25: Assessment Data Collection Menu

Button	Function
<b>Profile Organization</b>	Profile page 1 (Describe the Organization) are general questions about the program including type of assessment, phase in acquisition, contract, CAGE codes and locations of where the work is being performed.
<b>Scope Assessment</b>	Profile page 2 (Describe the Operating Environment) includes questions regarding specific detail of the program, type of information included and asset groups. The answers to these questions directly correlate to the required countermeasures.
<b>Identify Assets</b>	Identify specific assets in the program. (Assets have been pre-valued).
<b>Characterize Threats</b>	Confirm threats of program. (These have been pre-populated).
<b>Conduct Assessment</b>	Actual assessment questions based on the profile, assets and threats for the specific program; export and upload of questions.
<b>Finish and Lock</b>	Finish and lock a completed assessment.
<b>Back to Assessment Menu</b>	Return to Assessment Menu

Figure 26: Data collection icons and functions

## Profile Screens

### Profile Organization – Describe the Organization

This page asks general information about the program.

A red asterisk (\*) indicates the question is required. Blue information bubbles (i) indicate further information is available. (Click on the bubble to see the information).

**Describe the organization.**  
Please complete the following information to describe the organization. An asterisk (\*) indicates questions that require an answer to continue.

Your Assessment has been created. Please use the workflow to continue.

**Acquisition Security**

**These buttons are not used for ASM**

**Red asterisk indicates question is required**

**View Template Answers** **Revert All To Template Values**

**ASSESSMENT INFORMATION**

1. What is the program name?
- 1.a. If other, please type in the Program Name\*:
2. What type of assessment?
3. Who provided the information for the assessment?
- 3.a. Sub Name\*:

**PROGRAM INFORMATION**

4. Does the program have a Program Protection Plan?
- 4.a. If you are a PMO, please complete a PPP.

**Program Protection Plan**

**Click blue info bubbles for further information**

**PMO can complete PPP survey and have it linked to the PMO assessment.**

5. What ACAT level is this program?

Figure 27: Profile Page 1, Describe the Organization

**Profile Page 1- Describe the Organization, continued:**

**Operations and Sustainment Path:** Question 6, 7 and 8 are relative to the Operations and Sustainment path. Only one of the parent questions will be answered yes with the applicable child question answered. The remaining questions will be answered “No”.

OPERATIONS & SUSTAINMENT PATH - PLEASE SELECT YES TO APPLICABLE PATH AND ANSWER REMAINING NO

6. Is the program using Major Capability Acquisition?

7. Is the program using Urgent Capability Acquisition?

-- 6a. Milestone\*

-- 7a. Phase\*

-- 8a. Milestone\*

8. Is the program using Middle Tier of Acquisition?

Question 6, 7 and 8 are parent questions. 6a, 7a and 8a are child questions. Child questions are available to answer when the parent question is answered yes. Otherwise they are greyed out.

Only one of the scenarios applies. Select “Yes” to the one that applies and answer the child question. Answer the other two questions “No”.

\*\*\*UPDATE COMING SOON!\*\*\*\*This will be a single question

Q. Please list all Contract Numbers, CAGE codes, and locations of the Prime and other contractors (Prime CAGE code should be first row). [\(i\)](#)

Contract Number	Cage Code	Location
No records to view		

Populate this section by using the Add/Edit/Delete buttons

+ Add

Click Next Section/Tab when page is complete

< Previous Section/Tab

Figure 28: Profile Page 1 – Describe the organization, bottom of page

**Contract Numbers, CAGE codes and Locations:** The Describe the Organization page asks for contract numbers, CAGE codes and locations. There will be multiple rows for this section as information is learned. For example, for the first assessment, only the contract number may be known. In subsequent assessments, other information may be known. Populate and edit this section by using the Add/Edit/Delete buttons. *Note: This number could also be an RFP number.*

## Profile Page 1 Profile Page 1 – Describe the Operating Environment Drop Down menus

In this section, each of the drop choices is explained.

### Question 1: What is the Name of the Program?

Program names are listed alphabetically in the drop-down list. If your program is not listed, select “Other” and add the name in in question 1a.

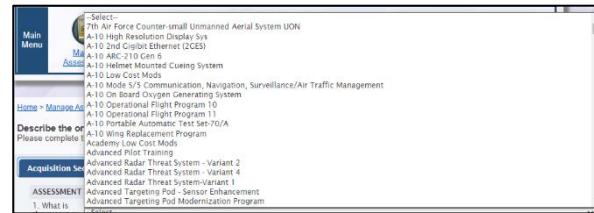


Figure 29: Drop down menu for Program names

### Question 2: What type of Assessment?

A program will have multiple assessments throughout the acquisition life cycle as represented by the list below. It is important to measure risk and follow trends throughout the life cycle. The table below defines the assessment type options and when to select each.

The type of assessment is relative to the stage in the process as shown below:

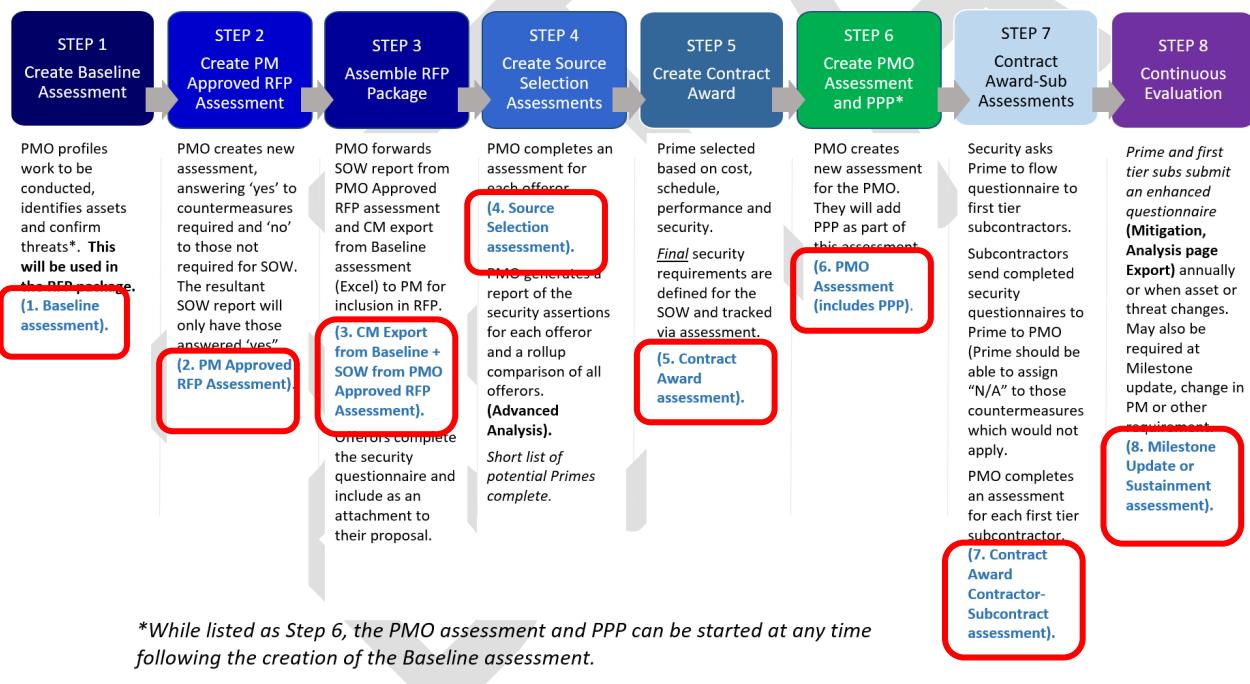


Figure 30: ASM Process

Option	Select when
Initial (Pre-RFP)	Creating the Baseline assessment
PM Approved RFP	Creating the adjusted assessment for inclusion in the RFP package.
Contract Award	Creating the assessment reflective of the actual security requirements in the contract.
PMO	Creating the Program Management Office Assessment (includes adding the Program Protection Plan)
Sustainment	Creating an assessment used to measure risk during the duration of a contract.
Milestone Update	Creating an assessment that has a different milestone than other assessments.

Figure 31: Profile page 1 – Describe the organization: Option and definitions of What Type of Assessment.

**Question 3: Who provided the information for the assessment?**

The PMO creates and inputs information on all assessments but the source of the information varies depending on the type of assessment. The table below shows when to select each option.

Question 3a. is only available when completing an assessment for a sub. The sib would be selected as the provider of information and the name of the sub would be entered in the text field.

Option	Select when
Prime Contractor	Uploading/inputting information from a contractor's completed assessment
Subcontractor	Uploading/inputting information from a subcontractor's completed assessment
Program Office	Creating the Baseline OR conducting a PMO risk assessment
Owner/Operator	Uploading information from an Owner/Operator

Figure 32: Profile page 1 – Options and definitions for Who provided the information for the assessment.

**Question 4: Does the program have a Program Protection Plan?**

Option	Select when
Yes	The program has an established PPP
No	The program does not have an established PPP

Figure 33: Profile page 1 – Options and definitions for “Does the program have a Program Protection Plan?”

**Button: Link to Program Protection Plan Survey**

**This is only used for the PMO assessment.** This button can be disregarded on all other assessments. As part of the PMO assessment, the PPP is added in association of the assessment. Users can use this link to go directly to a PPP. The newly created PPP is directly linked to the assessment. Users can go back and forth between the PPP and the assessment with no worry of losing data. **For more on this process, see Job Aide Step 6.**



Figure 34: Program Protection Plan button

**Question 5: What ACAT level is this program?**

ACAT levels are important in trend analysis. Select the applicable ACAT level for the program in accordance with the guidelines below. If the program does not fall under any of the below guisleines, select “Other” and add a description of the level.

Question 5a is only available if “Other is chosen. This question becomes available when the user selects “other” for ACAT level. This is a free form text field up to 4000 characters. Enter a description of the ACAT level and include a reason why it does not fall under the pre-defined levels.

Option	Select when	Decision Authority
ACAT I	<ul style="list-style-type: none"> <li>• Dollar value for all increments of the program: estimated by the DAE to require an eventual total expenditure for research, development, and test and evaluation (RDT&amp;E) of more than <b>\$480 million</b> in Fiscal Year (FY) 2014 constant dollars or, for procurement, of more than <b>\$2.79 billion</b> in FY 2014 constant dollars</li> <li>• MDA designation</li> <li>• Major Defense Acquisition Program (MDAP) (10 U.S.C. 2430 (Reference (n)))</li> </ul>	ACAT ID: DAE ACAT IB: SAE ACAT IC: Head of the DoD Component or, if delegated, the CAE
ACAT IA	<ul style="list-style-type: none"> <li>• Major Automated Information System (MAIS): A DoD acquisition program for an Automated Information System (AIS) (either as a product or a service) that is either:           <ul style="list-style-type: none"> <li>• Designated by the MDA as a MAIS program; or</li> <li>• Estimated to exceed:               <ul style="list-style-type: none"> <li>• <b>\$75 million</b> in FY 2014 constant dollars for all expenditures, for all increments, sprints, etc., regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operation, and sustainment, and incurred in any single FY; or</li> <li>• <b>\$400 million</b> in FY 2014 constant dollars for all expenditures, for all increments, sprints, etc., regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, operations and sustainment, and disposal, and incurred from the beginning of the Materiel Solution Analysis Phase through deployment at all sites; or</li> <li>• <b>\$815 million</b> in FY 2014 constant dollars for all expenditures, for all increments, sprints, etc., regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operations and maintenance, and incurred from the beginning of the Materiel Solution Analysis Phase through sustainment for the estimated useful life of the system.</li> </ul> </li> <li>• MDA designation as special interest</li> </ul> </li> </ul>	ACAT IAM: DAE ACAT IAC: CAE or as delegated
ACAT IAC	<ul style="list-style-type: none"> <li>• Major Automated Information System (MAIS): A DoD acquisition program for an Automated Information System (AIS) (either as a product or a service) that is either:           <ul style="list-style-type: none"> <li>• Designated by the MDA as a MAIS program; or</li> <li>• Estimated to exceed:               <ul style="list-style-type: none"> <li>• <b>\$75 million</b> in FY 2014 constant dollars for all expenditures, for all increments, sprints, etc., regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operation, and sustainment, and incurred in any single FY; or</li> <li>• <b>\$400 million</b> in FY 2014 constant dollars for all expenditures, for all increments, sprints, etc., regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, operations and sustainment, and disposal, and incurred from the beginning of the Materiel Solution Analysis Phase through deployment at all sites; or</li> <li>• <b>\$815 million</b> in FY 2014 constant dollars for all expenditures, for all increments, sprints, etc., regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operations and maintenance, and incurred from the beginning of the Materiel Solution Analysis Phase through sustainment for the estimated useful life of the system.</li> </ul> </li> <li>• MDA designation as special interest</li> </ul> </li> </ul>	CAE or as delegated
ACAT IC	<ul style="list-style-type: none"> <li>• Dollar value for all increments of the program: estimated by the DAE to require an eventual total expenditure for research, development, and test and evaluation (RDT&amp;E) of more than <b>\$480 million</b> in Fiscal Year (FY) 2014 constant dollars or, for procurement, of more than <b>\$2.79 billion</b> in FY 2014 constant dollars</li> <li>• MDA designation</li> <li>• Major Defense Acquisition Program (MDAP) (10 U.S.C. 2430 (Reference (n)))</li> </ul>	Head of the DoD Component or, if delegated, the CAE

Option	Select when	Decision Authority
<b>ACAT ID</b>	<ul style="list-style-type: none"> <li>Dollar value for all increments of the program: estimated by the DAE to require an eventual total expenditure for research, development, and test and evaluation (RDT&amp;E) of more than <b>\$480 million</b> in Fiscal Year (FY) 2014 constant dollars or, for procurement, of more than <b>\$2.79 billion</b> in FY 2014 constant dollars</li> <li>MDA designation</li> <li>Major Defense Acquisition Program (MDAP) (10 U.S.C. 2430 (Reference (n)))</li> </ul>	DAE
<b>ACAT IM</b>	<ul style="list-style-type: none"> <li>Dollar value for all increments of the program: estimated by the DAE to require an eventual total expenditure for research, development, and test and evaluation (RDT&amp;E) of more than <b>\$480 million</b> in Fiscal Year (FY) 2014 constant dollars or, for procurement, of more than <b>\$2.79 billion</b> in FY 2014 constant dollars</li> <li>MDA designation</li> <li>Major Defense Acquisition Program (MDAP) (10 U.S.C. 2430 (Reference (n)))</li> </ul>	
<b>ACAT II</b>	<ul style="list-style-type: none"> <li>Does not meet criteria for ACAT I or IA</li> <li>Major system (10 U.S.C. 2302d (Reference (h)))</li> <li>Dollar value: estimated by the DoD Component head to require an eventual total expenditure for RDT&amp;E of more than <b>\$185 million</b> in FY 2014 constant dollars, or for procurement of more than <b>\$835 million</b> in FY 2014 constant dollars</li> <li>MDA designation (10 U.S.C. 2302 (Reference (h)))</li> </ul>	CAE or the individual designated by the CAE
<b>ACAT III</b>	<ul style="list-style-type: none"> <li>Does not meet criteria for ACAT II or above</li> <li>An AIS program that is neither a MAIS program nor a business system</li> </ul>	Designated by the CAE
<b>Other</b>	Does not meet the criteria of any above	

Figure 35: ACAT levels

#### Question 6, 7 and 8. Operations and Sustainment Path

These three questions work together. You would only select “Yes” to one of the questions and add the applicable phase. The other two questions would be marked “No”. A program can only have one operations and sustainment path. The system will not prompt an error if more than one is answered “yes” but it will be incorrect on any generated reports. This is changing later this year to a single question.

Each question has a “Yes” or “No” answer. If answered “yes”, the child question asks which phase.

Path	Milestone
<b>Major Capability Acquisition</b>	Pre-MSA
	MS-A
	Pre MS-B
	MS-B
	Post MS-B
	Pre- MSC
	Post MS-C
<b>Urgent Capability Acquisition</b>	Pre-Development
	Development
	Production and Development
<b>Middle Tier of Acquisition</b>	MS-B
	MS-C
	Post MS-C

Figure 36: Operations and Sustainment Paths and Milestones

**Question 9: Contract number, CAGE code, location and Identification of Prime.**

This question is populated as information becomes known. It will have multiple rows as the program moves forward in the process. At least one column in a row must be completed to add information. For example, you may know the contract number but not the location. You can add the contract number without having to add the information in the other columns.

**9. Please list all Contract Numbers, CAGE codes, and locations of the Prime and other contractors (Prime CAGE code should be first row). [i](#)**

Contract Number	Cage Code	Location	Is this the Prime?

Use buttons to add, edit, delete or find.

+ Add    Edit    Delete    Refresh    Find    Page 1 of 0

Add new row

**Add New Record**

Contract Number

Cage Code

Location

Is this the Prime?

Figure 37: Adding contract numbers, CAGE codes and locations. This is also where the Prime is identified.

**Identification of the Prime:** Once a Prime has been selected, identify them by adding a “Yes” to the last column of the row with Prime information.

**9. Please list all Contract Numbers, CAGE codes, and locations of the Prime and other contractors (Prime CAGE code should be first row). [i](#)**

Contract Number	Cage Code	Location	Is this the Prime?
123456	8057	Littleton	No
123456			No
123456	9587	Justin	Yes

+ Add    Edit    Delete    Refresh    Find    Page 1 of 1    50    View 1 - 3 of 3

Figure 38: Contract number grid where Prime is identified.

n and included  
ple, if a program  
e “Yes” or “No”

In some cases, questions will not be available until a question above is answered yes. For example, if the program has no intelligence information, no further intelligence information is needed so the questions are grayed out and unavailable.

**Describe the operating environment.**  
Please answer the following questions about the operating environment to complete your profile. An asterisk (\*) indicates questions that require an answer to continue.

**Acquisition Security**

YOU MUST ANSWER QUESTIONS 1-6; ANSWER NO TO ALL BUTTON IS ONLY APPLICABLE TO TECHNOLOGY AREAS ⓘ

1. Does this program have classified information? *	Yes
-- 1.a. Is access to Critical Nuclear Weapon Design Information (CNWDI) required under this contract? *	--Select--
-- 1.b. Does this program contain Top Secret elements? *	--Select--
-- 1.b.1 Does this program contain SCI? *	--Select--
-- 1.c. Does this program contain Secret elements? *	--Select--
-- 1.d. Does this program contain Confidential elements? *	--Select--
-- 1.e. Is access to Foreign Government Information (FGI) required under this contract? *	--Select--
-- 1.f. Is access to Formerly Restricted Data (FRD) information required under this contract? *	--Select--
-- 1.g. Is access to intelligence information required under this contract? *	--Select--
-- 1.g.1 Is access to SCI intelligence information required under this contract? *	--Select--
-- 1.g.2 Is access to non-SCI intelligence information required under this contract? *	--Select--
-- 1.h. Does the contract require access to JWICS? *	--Select--
-- 1.i. Is access to NATO information required under this contract? *	--Select--
-- 1.j. Is access to Restricted Data (RD) information required under this contract? *	--Select--
-- 1.k. Does the contract require access to SIPRNet? *	--Select--
2. Is Controlled Unclassified Information (CUI)/Controlled Technical Information (CTI) expected for this program? *	Yes
-- 2.a. Will any part of the weapon system or networks supporting the development effort use removable media? *	--Select--
-- 2.b. Will the program have Operations Security (OPSEC) requirements? *	--Select--
3. Will Prime contractors have access to classified information? *	Yes
-- 3.a. In performing this contract, will the contractor fabricate, modify, or store classified hardware? *	--Select--
4. Is Critical Program Information (CPI) present or expected on the program? *	Yes
-- 4.a. Does the program have inherited CPI? *	--Select--
-- 4.b. Will any part of the weapon system or networks supporting the development effort use removable media? *	--Select--
-- 4.c. Will the program have Operation Security (OPSEC) requirements? *	--Select--
5. Does the program or weapon system employ components/parts that are subject to the Supply Chain Risk Management (SCRIM) process and its federally-mandated policies? *	Yes
6. Do you have Trusted Systems Network (TSN) Defense Federal Acquisition Regulation Supplement (DFARS) clause on contract? *	Yes
-- 6.a. Will any component store or transmit any classified information? *	--Select--

These questions are  
grayed out until the first  
question (parent  
question) is answered  
“yes”.

Figure 39: Profile page 2 (Describe the Operating Environment, top of page)

## Profile Page 2, Describe the operating Environment, continued – Technology Areas - Asset Groups

The ASM has 335 assets derived from IBTL, HPG, DoD, Restricted Counter Low Observables (CLO), Restricted Low Observables (LO) Technologies, Tier 1 Technology, Tier 2 Technology, and Air Force assets. The source of the asset category is in parentheses. For example, if the asset category Aeronautics Systems (IBTL) is marked ‘Yes’, the asset list on the Assets page will include IBTL assets in this category.

For profile page 2, users select the applicable asset groups for the program. Once all included groups are selected, click on “**Answer No to all unanswered**” to mark the remaining groups as “No”. (This saves keystrokes and time as you create the assessment).

**TECHNOLOGY AREAS (ANSWER NO TO ALL BUTTON IS APPLICABLE HERE)**

**Answer 'No' to All Unanswered**

Click on Answer 'No' to All Unanswered after all asset groups selected.

7. Select the asset categories that are applicable for your program.

Item
<input checked="" type="radio"/> Yes <input type="radio"/> No Aeronautic Systems (IBTL)
<input checked="" type="radio"/> Yes <input type="radio"/> No Agricultural Technology (IBTL)
<input checked="" type="radio"/> Yes <input type="radio"/> No Armament and Survivability (IBTL)
<input type="radio"/> Yes <input checked="" type="radio"/> No Biological Information or Technology (IBTL)
<input type="radio"/> Yes <input checked="" type="radio"/> No Chemical Information or Technology (IBTL)
<input type="radio"/> Yes <input checked="" type="radio"/> No Command, Control, Communication, And Computer (C4) (IBTL)
<input type="radio"/> Yes <input checked="" type="radio"/> No Directed Energy (IBTL)
<input type="radio"/> Yes <input checked="" type="radio"/> No Electronics (IBTL)
<input type="radio"/> Yes <input checked="" type="radio"/> No Emerging Technology (IBTL)

Rows 1 - 43 of 43

< Previous Section/Tab | Exit to Data Collection/Lock | Next Section/Tab >

Figure 40: Profile page 2 – Scope the Assessment – Questions

**NOTE: Profile Page 2:** The ‘Answer ‘No’ to All Unanswered’ button is only relative to the asset groups. Each of the questions above must be answered individually. The ‘Answer ‘No’ to All’ button does not affect the questions- only the asset groups.

## Asset Page

**We need to ask you a few questions about your assets.**  
 Your answers will help us identify which assets must be protected. Use the "Filter by Category" dropdown to filter the asset list. To annotate an individual response (or view an annotation), select a row to highlight, then select "Add/View Comment". If you choose to enter a comment, enter text and save. Once saved, an icon will display in the Comment column indicating text has been entered. For additional information about an item, double click on the row to view. The previous and next buttons will route you to either the previous or the next section.

Note: Any listing containing more than 50 items must be expanded at the bottom center of the grid to display additional rows.

< Previous Section/Tab	Exit to Data Collection/Lock	Next Section/Tab >																			
Revert All To Template Values	Answer 'No' to All Unanswered	Add/View Comment	Duplicate Selected Asset																		
Remove Duplicated Asset	Export to Excel	Upload Responses																			
Revert Selected to Template Value																					
Filter by Category All Categories 0 / 82			Overall Progress: 0 Answered / 82 Required																		
<b>Assets - Double click row for more information</b> <table border="1"> <thead> <tr> <th>Category</th> <th>Type</th> <th>Name</th> <th>Applicable?</th> <th>Criticality</th> <th>Score</th> <th>Comm</th> <th>Template I</th> <th>Objective(s)</th> </tr> </thead> <tbody> <tr> <td>Aeronautic Systems</td> <td>Aircraft &amp; Design</td> <td></td> <td>All</td> <td>SIGNIFICANT</td> <td>75</td> <td></td> <td></td> <td>Acquisition Security</td> </tr> </tbody> </table>				Category	Type	Name	Applicable?	Criticality	Score	Comm	Template I	Objective(s)	Aeronautic Systems	Aircraft & Design		All	SIGNIFICANT	75			Acquisition Security
Category	Type	Name	Applicable?	Criticality	Score	Comm	Template I	Objective(s)													
Aeronautic Systems	Aircraft & Design		All	SIGNIFICANT	75			Acquisition Security													

Figure 41: Assets Page

Assets show according to the categories selected on the Scope Assessment page (previous screen, Describe the Operating Environment).

Assets are pre-scored in accordance with DCSA asset criticality guidelines. Users can change the score if needed but must add a reason for the change.

The asset page has several buttons and functions to help make the process more efficient. The table below explains each button and their function:

Button	Function	Used for
Previous Section Tab	Returns to previous screen (Describe the Operating Environment)	Returning to previous screen to make changes or view
Next Section/Tab	Moves to Next Screen (Threats)	Moving to next screen (Threats) once asset screen is complete.
Exit to Data collection/Lock	Returns to Assessment main menu	Skipping screens and returning to main menu
Answer No to All Unanswered	Answers all unanswered assets "No"	Applicable assets have been selected as "Yes"
Add/View Comment	Pop up screen to add or view comment on an asset	Add or view a comment on a selected asset
Duplicate Selected Asset	Creates an asset with the same value as the selected asset	Adding an asset not listed
Remove Duplicated Asset	Deletes selected asset (only functional for duplicated assets)	Removing an asset added
Revert to Template Value	Disregards changes and reverts asset criticality value to the value in the template	Return asset value to template answer when a value was changed by mistake

Button	Function	Used for
Export to Excel	Exports the asset list into an Excel file	Creating a file to be shared for a group discussion or to make asset selection and value more efficient
Upload Responses	Uploads the completed asset list into ASM	Uploading all asset answers with more efficiency

Figure 42: Asset Page button functions 1

## Asset Page, Additional Functionality

The asset page also has additional functions as follows:

- Double click on any asset to get further information on the asset.
- Filter by Asset Category enables the user to filter the list by category.
- Filter boxes above each column enables the user to quickly find an asset.
- Overall progress shows the number required to be answered and the number answered.
- Info bubble (blue round button) shows the template value.

The screenshot shows the 'Assets' page with several annotations:

- Navigation and function buttons:** A yellow box highlights the top navigation bar with buttons like < Previous Section/Tab, Exit to Data Collection/Lock, Navigation and function buttons, Next Section/Tab >, Revert All To Template Values, Answer 'No' to All Unanswered, Add/View Comment, Duplicate Selected Asset, Remove Duplicated Asset, Export to Excel, and Upload Responses.
- Filter by Category:** A red box surrounds the 'Filter by Category' dropdown menu set to 'All Categories 0 / 82'. A yellow box labeled 'Assets can be filtered by category' is positioned above it.
- Assets Grid:** The main area displays a grid of assets. A red box highlights the first row: 'Aeronautic Systems' under Category, 'Aircraft & Design' under Type, and '75' under Criticality. A blue info bubble next to '75' says 'Assets have pre-scored criticality. Blue info bubble shows template criticality (default scores)'.
- Asset Details:** A red box highlights the details for the first asset: 'Asset Details - Aircraft & Design', 'What is this?', 'Per the IBTL, Aeronautic Systems include combat and noncombat air vehicle designs and capabilities.', 'How could an adversary collect/exploit this?', 'Aircraft Design is vulnerable to Request for Information/Solicitation; Attempted Acquisition of Technology; Exploitation of Business Activities; Surveillance', 'Specific critical assets in this category includes, but is not limited to...', 'Asset Criticality: SIGNIFICANT (September 2019)', and 'Yes' and 'No' buttons.
- Information Bubbles:** Two blue info bubbles provide instructions: one pointing to the '75' criticality score and another pointing to the 'Yes' button.
- Group Selection:** A red box highlights the bottom of the grid with the text 'Assets show based on groups selected on previous page. Click on "Yes" to an asset to add.'

Figure 43: Asset Page in Detail

## Asset Selection Screen

When a user clicks on the ‘Yes’ button next to an asset, a pop-up display asks if the default value has been changed. If there are no changes, click on **Submit**.

If there are changes to an asset value:

- Use the drop-down menu to **select the criticality**
- **Select “Yes”** to the next question (indicating you did make changes)
- **Provide a reason** for the change.
- Click **Submit** to save changes.

The asset is shown below in accordance with the following parameters:

**Nominal:** The transfer of developed or in development U.S. technology and information is unlikely, and would cause NOMINAL damage to national security. The asset is of LOW importance to the adversary.

**Limited to Moderate:** The transfer of developed or in development U.S. technology and information has a chance of occurring, and could cause LIMITED TO MODERATE damage to national security. The asset is of MEDIUM importance to the adversary.

**Significant:** The transfer of developed or in development U.S. technology and information is likely and could cause SIGNIFICANT damage to national security. The asset is of HIGH importance to the adversary.

**Critical:** The transfer of developed or in development U.S. technology and information is imminent and could cause SEVERE damage to national security. The asset is of CRITICAL importance to the adversary.

The recommended criticality is shown here. You can change this applicable to your program. If you change it, please add a reason.\*

Assets have pre-scored criticality.

Enter the reason for the default score changes.

Any changes to the value require a reason for the change

Click on Submit when done.

Submit Cancel

Figure 44: Changes to Asset Value

## Changes to Template Answers

Any deviations from template answers results in a red exclamation point next to the item. *This is not an error.* It is marked to highlight values different from the template.

Aeronautic Systems	Fixed Wing Combat Aircraft	Yes	No	SIGNIFICANT	75	?	Acquisition Security
				Yes	No	! LIMITED TO MODERATE	50
				Acquisition Security			

Deviations from the template will result in a red exclamation point. This is to highlight where changes occurred. This is not an error

Figure 45: Asset value changed showing red exclamation point.

## Adding a Missing Asset

In the event a program has an asset not shown in list, users can add an asset by duplicating an asset closest to the missing asset.

For example, if there is an asset resembling a fixed wing aircraft but is different enough to warrant an added item, users can add the missing asset by duplicating the fixed wing combat aircraft. They would then add name and criticality. The figure below shows the steps.

**To add an asset not listed, find the asset closest to the missing asset. The selected row shows in yellow.**

**Add the name of the asset and save.**

**Asset now shows in list. Click on "Yes" to add criticality and reason for addition.**

**Asset now shows in list with criticality. Red exclamation point indicates this is a deviation from the template.**

Figure 46: Adding an asset not listed.

Once all assets have an answer, click on **Next Section/Tab** to continue to the Threats page.

## Using Excel to Complete the Asset Page (Export to Excel)

If there are many assets or a working group will work on the asset list together, you can export the list into Excel and use Excel to complete the asset list. Once completed, you can use the Upload functionality to upload the completed Excel file. This can improve efficiency when there are many assets.

When completing, indicate whether the asset is included by adding yes or no into column E. If you change an asset's criticality value, you would provide a reason in column G.

A red cell indicates a required answer is missing.

The figure below shows the steps to export the Asset list.

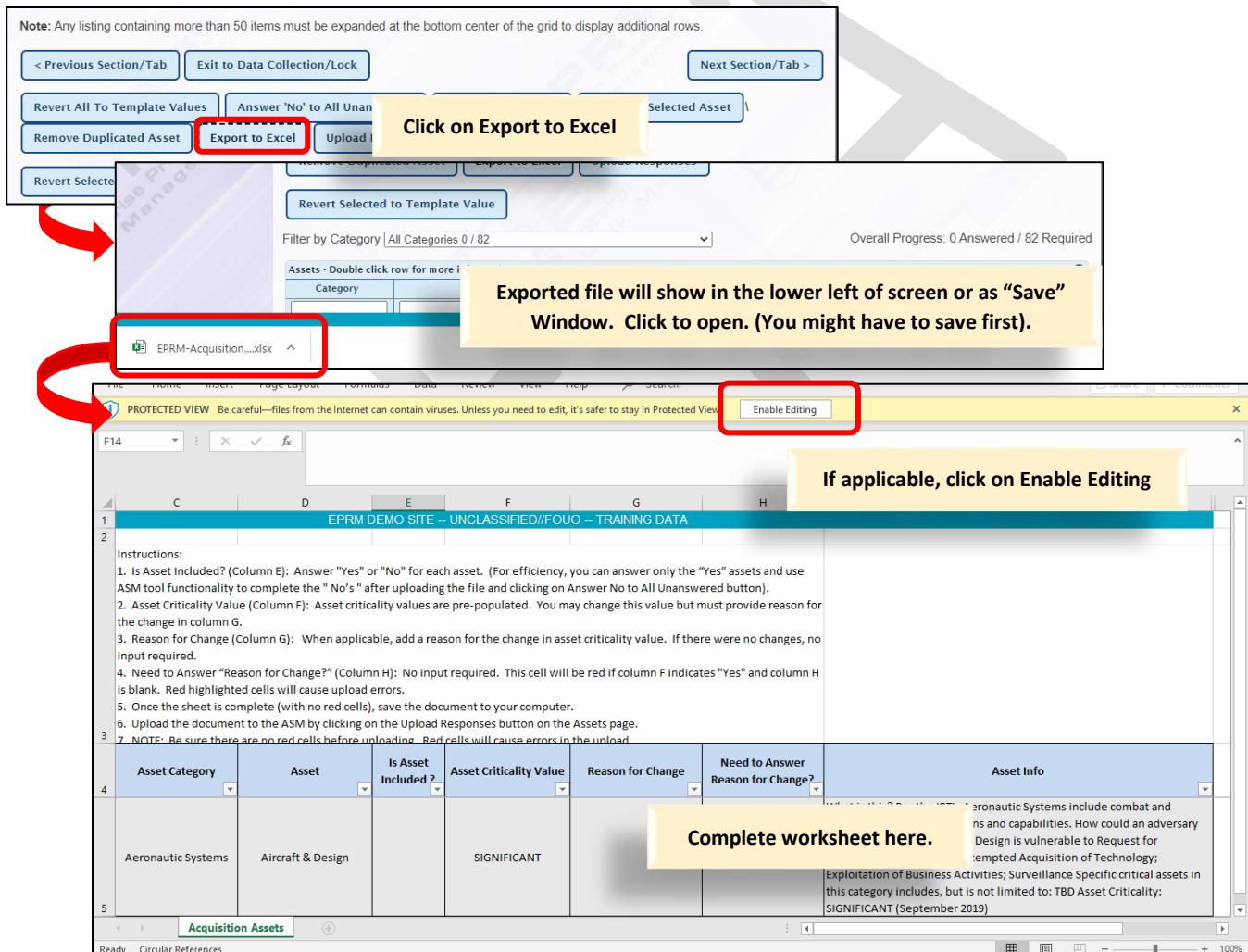


Figure 47: Exporting an Asset List

## Upload the Assets (upload Responses)

Once the asset list is complete, use the Upload Responses button to populate the assets page.

Click on Upload responses, browse for the file and select it. Click on upload and it will upload all responses. To return to the Asset page, click on the Back button.

The figure below shows the steps to uploading a completed asset file.

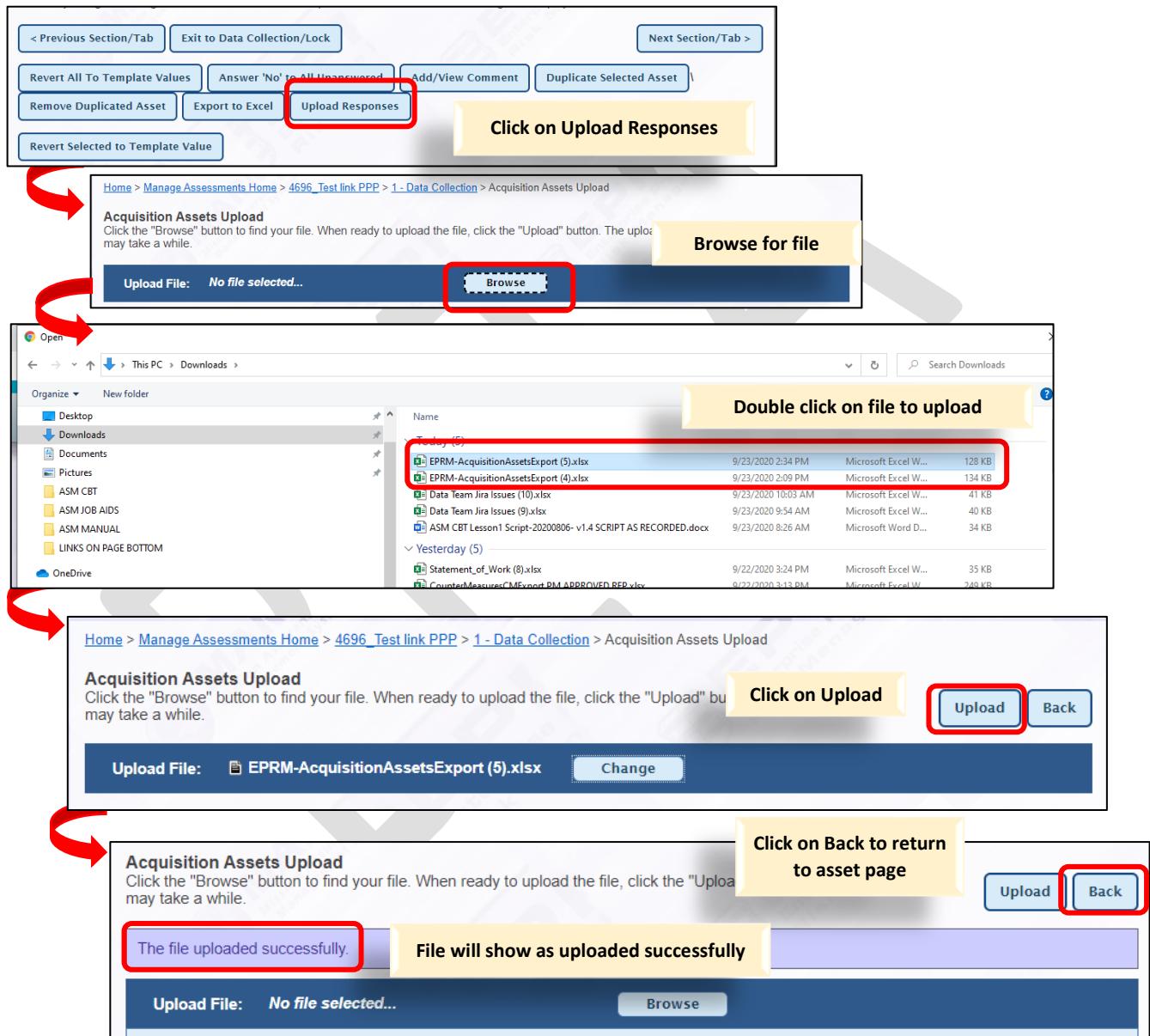


Figure 48: Steps to upload a completed asset file

## Threat Page

Like assets, threats are pre-scored according to the DCSA threat criticality recommendations. You may change a threat level but will need to provide a reason for the change. You may also add a missing threat by using the Duplicate Selected Threat button. This functionality is the same in threats as it is in the Assets page. Any deviation from the template answers will result in a red exclamation point next to the item.

In most cases, users will click on **Next Section/Tab** on the threats page.

**ASM USERS: CLICK ON THE NEXT SECTION/TAB BUTTON TO CONTINUE.**

Threat data has been pre-populated with values from DCSA. Any change to these values requires an explanation and rationale.

**Note:** Any listing containing more than 50 items must be expanded at the bottom center of the grid to display additional items.

< Previous Section/Tab    Exit to Data Collection/Lock    Next Section/Tab >

Revert All To Template Values    Answer 'No' to All Unanswered    Add/View Comment    Duplicate Selected Threat

Remove Duplicated Threat    Revert Selected to Template Value

Filter by Source  
All Sources 15 / 15

Filter by Method  
All Methods 15 / 15

You can filter by Source or Method or both

Threat page functionality works the same as the asset page.

Overall Progress: 15 Answered / 15 Required

Source	Method	Name	Applicable?	Rating	Score	Comm	Template In	Objective(s)
Conference, Conventions, or Tradeshows	Exploitation of Experts		Yes    No	Medium-Low	0.18			Acquisition Security
Conference, Conventions, or Tradeshows	Exploitation of Supply Chain		Yes    No	Low	0.05			Acquisition Security
Conference, Conventions, or Tradeshows	Request for Information/Solicitation		Yes    No	High	0.93			Acquisition Security

Figure 49: Threat page.

**NOTE: Threats are pre-selected with pre-determined scores based on the assets chosen. In almost all cases, you will click on Next Section/Tab. If you need to change a threat value, you can but it requires a detailed reason for the change.**

## Threat Option Buttons

The Threat option buttons have the same functionality as in other pages. The table below provides a brief description of each button.

Button	Function	Used for
<b>Previous Section Tab</b>	Returns to previous screen (Describe the Operating Environment)	Returning to previous screen to make changes or view
<b>Next Section/Tab</b>	Moves to Next Screen (Threats)	Moving to next screen (Threats) once asset screen is complete.
<b>Exit to Data Collection/Lock</b>	Returns to Assessment main menu	Skipping screens and returning to main menu
<b>Answer No to All Unanswered</b>	Answers all unanswered assets "No"	Applicable assets have been selected as "Yes"
<b>Add/View Comment</b>	Pop up screen to add or view comment on an asset	Add or view a comment on a selected asset
<b>Duplicate Selected Threat</b>	Creates an asset with the same value as the selected asset	Adding an asset not listed
<b>Remove Duplicated Threat</b>	Deletes selected asset (only functional for duplicated assets)	Removing an asset added
<b>Revert to Template Value</b>	Disregards changes and reverts asset criticality value to the value in the template	Return asset value to template answer when a value was changed by mistake

Figure 50: Threat Option Buttons 1

## Threat Changes - \*\*\*Requires detailed reason\*\*\*

To make a change in the threat level:

- Click on the “Yes” button of the threat.
- Select the **new threat level**.
- Click on **Add/View comment**.
- Add **comment**.

The figure on the following page shows the steps for changing a threat level.

**Threats - Double click row for more information**

Source	Method	Name	Applicable?	Rating	Score	Comment	Template Inv	Objective(s)
Conference, Conventions, or Tradeshows	Attempted Acquisition of Technology		All	Low				
<b>Threat Matrix - Conference, Conventions, or Tradeshows - Attempted Acquisition of Technology</b> Use the matrix below to help establish the severity of Attempted Acquisition of Technology Conference, Conventions, or Tradeshows for your organization. SME: Please add instructions if you wish								
Adversary US Loss of Critical information could have MINOR impact on the program. Loss of Critical information could have MODERATE impact on the program. Loss of Critical information could have APPRECIABLE impact on the program. Loss of Critical information could have SERIOUS impact on the program. Loss of Critical information could have SEVERE impact on the program.								
Of CRITICAL importance to the adversary. Obtaining the information considerably contributes to meeting the adversary's objective.								
Of such CRUCIAL importance to the adversary. Obtaining the information appreciably contributes to the adversary's objective.								
Of such ESSENTIAL importance to the adversary. Obtaining the information greatly contributes to meeting the adversary's objective.								
Of MODERATE importance to the adversary. Obtaining the information contributes to meeting the adversary's objective.								
Of MINOR importance to the adversary.								
Medium-High Medium-High Medium-High Medium-High High Medium Medium Medium-High Medium-High Medium-High Low Medium-Low Medium Medium Medium-High Low Low Medium-Low Medium-Low Medium-High Low Low Low Low Medium-High								

To change a threat value, click on the "Yes" button next to the threat to be changed.

Click on the value for the threat.

< Previous Section/Tab    Exit to Data Collection/Lock    Next Section/Tab >

Revert All To Template Values    Answer 'No' to All Unanswered    Add/View Comment    Duplicate Selected Threat

Revert Selected to Template Value

Filter by Source  
All Sources 30 / 30

Overall Progress: 30 Answered / 30 Required

**Threats - Double click row for more information**

Source	Method	Name	Applicable?	Rating	Score	Comment	Template Inv	Objective(s)
Conference, Conventions, or Tradeshows	Attempted Acquisition of Technology		All	Yes	No	Medium	0.48	Acquisition Security
<b>Threat Comment</b> Conference, Conventions, or Tradeshows - Attempted Acquisition of Technology Enter your comment. Bulletin DF568 - threat level changed from low to medium 3944 characters remaining (max 4000)								
Yes No Medium 0.48 Acquisition Security								

Add a reason for the change in the comment field.

Red exclamation mark will indicate a threat has been changed from the template value.

Threat now shows as being changed with comment.

Figure 51: Changing a threat value.

## Countermeasures Page

The countermeasures page is the list of recommended countermeasures (in the form of questions) based on the program description, operating environment, assets and threats. Every program may have a different set of countermeasures. i.e., given this program in this environment with these assets and threats, these countermeasures are recommended.

Each question has an associated weight depending on how well it reduces vulnerability. Countermeasures technical and preventive in nature will have a higher weight than those considered administrative.

**Your answers will help us better understand your current vulnerabilities.**  
Your answers will help us better understand your current vulnerabilities. Use the "Filter by Category" dropdown to filter the list. To complete a non-applicable (N/A) answer, you will be required to enter text in a comment field indicating the reason for this response. You may also select "Answer No to All Unanswered" to facilitate rapid population of multiple No responses. To annotate an individual response (or view an annotation), select a row to highlight, then select "Add/View Comment". If you choose to enter a comment, enter text and save. Once saved, an icon will display in the Comment column indicating text has been entered. For additional information about an item, double click on the row to view. The previous and next buttons will route you through the assessment data collection.

Note: Any listing containing more than 50 items, must be expanded at the bottom center of the grid to display additional rows.

To print the full listing, use the "Export to Excel" button to export the list to an excel file, which can then be sorted and formatted to your individual preferences.

< Previous Section/Tab    Exit to Data Collection/Lock    Next Section/Tab >

Export to Excel    Upload Responses    Revert All To Template Values    Answer 'No' to All Unanswered

Add/View Comment

Revert Selected to Template Value

For this program scenario, there are 122 parent countermeasures recommended and 41 child countermeasures. (Child countermeasures only show if the parent question is answered "Yes").

Overall Progress: 0 Answered / 122 Required (163 Total)

Countermeasures/Benchmarks - Double click row for more information

Category	Countermeasure/Benchmark	Answer	Comment	Template Info	Objective(s)
CLASSIFIED - Classified Critical Nuclear Weapon Design Information (CNWDI) - 01	Do personnel meet the minimum requirements for access to CNWDI?	Yes    No    N/A			Acquisition Security
CLASSIFIED - Clearance and Safeguarding - 02	Why is this important? It is important the program and its subcontractors meet the minimum requirements to allow access to CNWDI to ensure no personnel that have the minimum access receives the information. This helps prevent unauthorized disclosure, loss or compromise of CNWDI.	N/A			Acquisition Security
CLASSIFIED - Clearance and Safeguarding - 03	Contracting Officer approval is required prior to granting CNWDI access to a subcontractor. Special briefings and procedures are also required. Access to CNWDI requires a final U.S. Government clearance at that appropriate level. This helps prevent authorized disclosure, loss or compromise of classified information.	N/A			Acquisition Security
CLASSIFIED - Clearance and Safeguarding - 04					Acquisition Security
CLASSIFIED - Clearance and Safeguarding - 05	Are personnel properly cleared for Confidential access?				Acquisition Security
CLASSIFIED - Foreign Government Information - 01	Do personnel meet the minimum requirements for access to Foreign Government Information (FGI)?	Yes    No    N/A			Acquisition Security
CLASSIFIED - Foreign Government	If awarded, does the program understand subcontractors may only be allowed access to FGI?	Yes    No    N/A			Acquisition Security

Double click on any countermeasure to get further information

Adjust list here.

< Previous Section/Tab    Exit to Data Collection/Lock    Next Section/Tab >

Figure 52: Countermeasure page.

## Child Questions

Some countermeasure questions, when answered “Yes”, will prompt other questions. These are parent questions. When the parent question is answered “Yes”, the resultant questions are called child questions. Child questions are not available until the parent questions are answered “yes”.

CLASSIFIED - Foreign Government Information - 03	Does the program have cleared facilities to access Foreign Government Information (FGI)?	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A		Acquisition Security
CLASSIFIED - Foreign Nationals - 01	Are Foreign Nationals anticipated to be involved in the program?	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A		Acquisition Security
CLASSIFIED - Foreign Nationals - 01.a	Does the program acknowledge that under 10 U.S.C. 2536(a), no DoD contract under a national security program may be awarded to an entity controlled by a foreign government if that entity requires access to proscribed information?	Not available until parent countermeasure is answered		Acquisition Security
CLASSIFIED - Formerly Restricted Data - 01	Do personnel meet the minimum requirements to allow access to Formerly Restricted Data (FRD) information?	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A		Acquisition Security
CLASSIFIED - Intelligence - 01	Do the program, Prime, Sub Contractors meet the minimum requirements for access to intelligence	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A		Acquisition Security

question.

Figure 53: Parent and Child Questions

## Countermeasure Option Buttons

Button	Function	Used for
Previous Section Tab	Returns to previous screen (Describe the Operating Environment)	Returning to previous screen to make changes or view
Next Section/Tab	Moves to Next Screen (Threats)	Moving to next screen (Threats) once asset screen is complete.
Exit to Data Collection/Lock	Returns to Assessment main menu	Skipping screens and returning to main menu
Answer No to All Unanswered	Answers all unanswered assets “No”	Applicable assets have been selected as “Yes”
Add/View Comment	Pop up screen to add or view comment on an asset	Add or view a comment on a selected asset
Duplicate Selected Threat	Creates an asset with the same value as the selected asset	Adding an asset not listed
Remove Duplicated Threat	Deletes selected asset (only functional for duplicated assets)	Removing an asset added
Revert to Template Value	Disregards changes and reverts asset criticality value to the value in the template	Return asset value to template answer when a value was changed by mistake
Export to Excel	Exports the list of countermeasures into a customized Excel file.	Completing the countermeasure questions in Excel (to improve efficiency). This is also the file sent to offerors to complete as part of their RFP response.
Upload Responses	Upload a completed Excel file of countermeasures.	Improving efficiency when answering countermeasures.

Figure 54: Countermeasure Option Buttons

Like the asset and threat pages, the countermeasure buttons have the same functionality as in other pages. The table below provides a brief description of each button.

### Export to Excel Functionality

A more efficient way to answer countermeasures is to export the file and answer them in Excel. This functionality also enables the user to create a file for offerors to complete and return with their RFP responses.

The figure below shows the steps to export the countermeasure file.

**Your answers will help us better understand your current vulnerabilities.**

Your answers will help us better understand your current vulnerabilities. Use the "Filter by Category" dropdown to filter the list. To complete a non-applicable (N/A) answer, you will be required to enter text in a comment field indicating the reason for this response. You may also select "Answer No to All Unanswered" to facilitate rapid population of multiple N/A responses. To annotate an individual response (or view an annotation), select a row to highlight, then select "Add/View Comment". If you choose to enter a comment, enter text and save. Once saved, an icon will display in the Comment column indicating text has been entered. For additional information about an item, double click on the row to view. The previous and next buttons will route you through the assessment data collection.

Note: Any listing containing more than 50 items, must be expanded at the bottom center of the grid to display additional rows.

To print the full listing, use the "Export to Excel" button to export the list to an excel file, which can then be sorted and formatted to your individual preferences.

< Previous Section/Tab   Exit to Data Collection/Lock   Next Section/Tab >

Export to Excel   Upload Responses   Add/View Comment   Revert Selected to Template Value

Click on the Export to Excel button on the countermeasures page.

Filter by Category All Categories 0 / 122 / 163

Do you want to open or save CounterMeasuresCMEExport.xlsx from demo.countermeasures.com?

Save   Save as   Save and open

Save as

Save and open

The Excel file has all the functionality of Excel. Items shown in red are required questions.

Category	Question	Answer	Answer Required	Comment	Info
CLASSIFIED - Classified Critical Nuclear Weapon Design Information (CNWDI) - 01	Do personnel meet the minimum requirements for access to CNWDI?		Yes No N/A		Why is this important? It is important the program and its subcontractors meet the minimum requirements to allow access to CNWDI to ensure only personnel that have the minimum access receives the information helps prevent the unauthorized disclosure, loss or compromise of CNWDI. Contracting Officer approval is required prior to granting CNWDI access to a subcontractor. Special briefings and procedures are also required to access CNWDI. Access to CNWDI requires a final U.S. Government clearance at that appropriate level. This helps prevent unauthorized disclosure, loss or compromise of classified information. How do I check this? Verify security is in compliance with the appropriate reference and authoritative guidance. References(s): References(s): S220.22, Volume 2, paragraph 5.1, 1 August 2018; DOD 5220.22-M (NISPM) Appendix D, 26 February 2006, Incorporating Change 2, 18 May 2016.
CLASSIFIED - Clearance and Safeguarding - 02	Are personnel properly cleared for SCI access?	Yes No N/A			Why is this important? Sensitive compartmentalized information (SCI) is classified information derived from intelligence sources, methods, or analytical processes that is required to be handled within access control systems established by the Director of National Intelligence. SCI shall be safeguarded in accordance with the policies and procedures of the DoD as implemented in DOD 5220.22-M (Ref. 1) and other applicable guidance. SCI requires extra protection above a top secret security clearance. It has to have special handling, which involves controls to access. All SCI matters shall be referred to the SS SSO may be designated as the activity security manager if the grade requirements for the position are met; however, the activity security manager cannot function as the SSO unless so designated by the cognizant intelligence official. How do I check this? To verify clearance levels, check the listing in JPA (Reference) S220.22, Volume 2, paragraph 5.1, 1 August 2018; NIST Special Publication 800-53 Revision 4, Appendix F (6), 22 January 2015; NIST Special Publication 800-53A Revision 4, Appendix F (PS-3; P5-6), 18 December 2015; S220.22-M (NISPM) Section 9-300 and Appendix D 26 February 2006, Incorporating Change 2, 18 May 2016.
CLASSIFIED - Clearance and Safeguarding - 03	Are personnel properly cleared for Top Secret access?	CMEExport			Why is this important? Top Secret information is classified as TOP SECRET if an unauthorized disclosure o

Figure 55: Exporting the countermeasures to Excel.

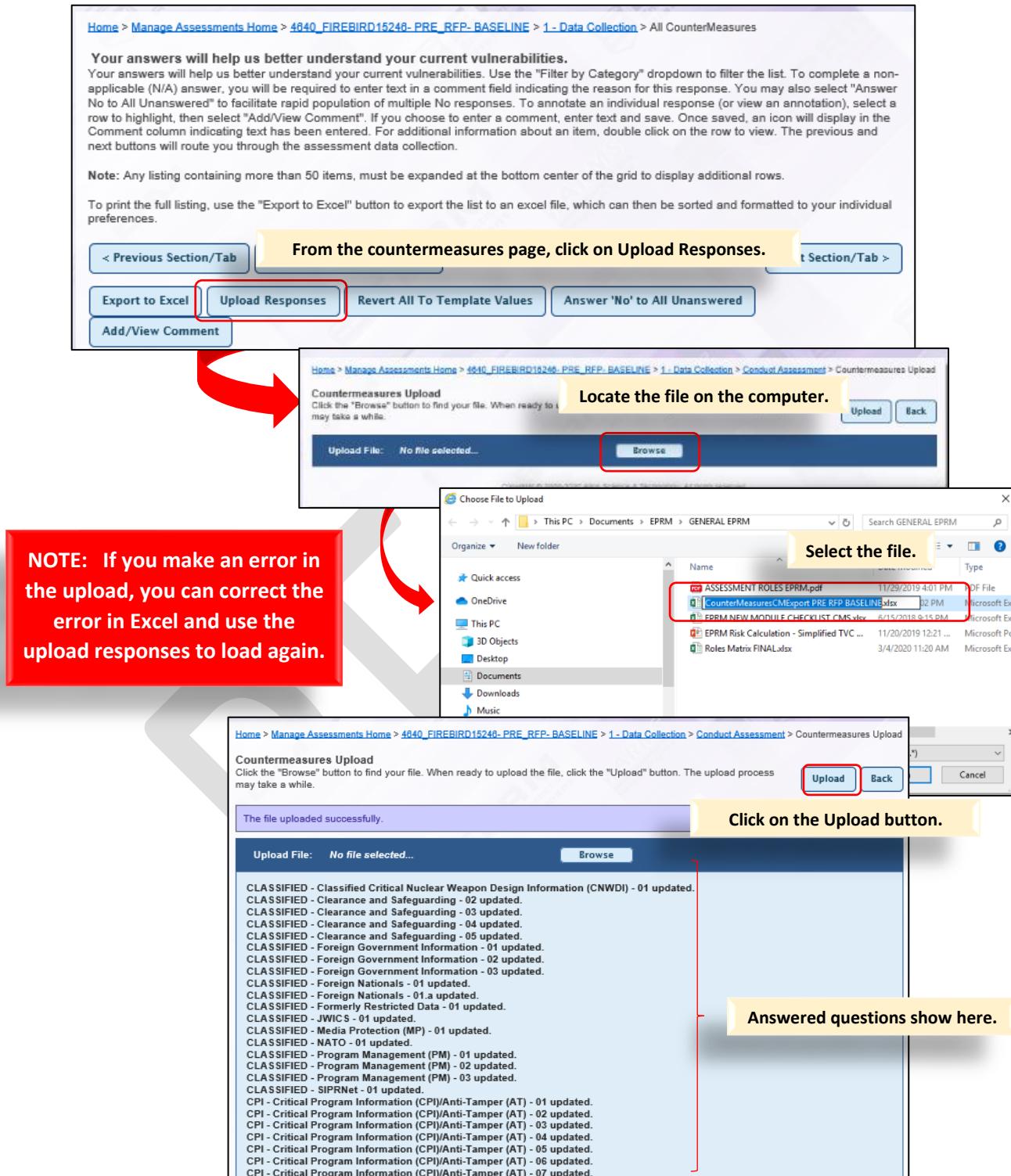


Figure 56: Uploading Responses to countermeasures (assessment questions).

Once Excel file has been uploaded, the countermeasures will show as answered.

Click on **Next Section/Tab** to return to assessment main menu.

Countermeasures/Benchmarks - Double click row for more information						
Category	Countermeasure/Benchmark	Answer	Comment	Template Info	Objective(s)	
CLASSIFIED - Classified Critical Nuclear Weapon Design Information (CNWDI) - 01	Do personnel meet the minimum requirements for access to CNWDI?	<input checked="" type="button"/> Yes <input type="button"/> No <input type="button"/> N/A			Acquisition Security	
CLASSIFIED - Clearance and Safeguarding - 02	Are personnel properly cleared for SCI access?	<input checked="" type="button"/> Yes <input type="button"/> No <input type="button"/> N/A			Acquisition Security	
CLASSIFIED - Clearance and Safeguarding - 03	Are personnel properly cleared for Top Secret access?	<input checked="" type="button"/> Yes <input type="button"/> No <input type="button"/> N/A			Acquisition Security	
CLASSIFIED - Clearance and Safeguarding - 04	Are personnel properly cleared for Secret access?	<input checked="" type="button"/> Yes <input type="button"/> No <input type="button"/> N/A			Acquisition Security	
CLASSIFIED - Clearance and Safeguarding - 05	Are personnel properly cleared for Confidential access?	<input checked="" type="button"/> Yes <input type="button"/> No <input type="button"/> N/A			Acquisition Security	
CLASSIFIED - Foreign Government Information - 01	Do personnel meet the minimum requirements for access to Foreign Government Information (FGI)?	<input checked="" type="button"/> Yes <input type="button"/> No <input type="button"/> N/A			Acquisition Security	
CLASSIFIED - If awarded, does the program understand						

Figure 57: Countermeasure page after Upload Responses completed.

**NOTE:** Countermeasures should be answered "Yes" or "No". If "N/A" is used, the user will need to provide a comment on why the countermeasure is not applicable.  
 "N/A" countermeasures are removed from the risk equation.

## Finish and Lock Assessment

Once assessment is complete, users click on the Finish and Lock Assessment to complete the assessment.



Figure 58: Finish and lock assessment.

*The rest of this page intentionally left blank.*

## Basic Analysis, Mitigation and Submission Page

### Risk Tab

Once an assessment is finished and locked, the Basic Analysis, Mitigation and Submission icon is available to view the risk and compliance of the completed assessment. This functionality is for the user to see the risk on a single assessment. Risk is based on an algorithmic calculation taking into account assets, threats and implemented countermeasures.

The screenshot displays the 'Basic Analysis, Mitigation and Submission' page for an assessment titled '4640\_FIREBIRD15246-PRE\_RFP-BASELINE'. The page is divided into several sections:

- Main Menu:** Includes icons for Manage Assessments, Advanced Analysis, Manage Templates (including AHTAs), Manage Survey Responses, View References and Materials, Legacy CVAMP Assessment Data, Manage MA Assessments, and Manage IAS.
- Assessment Workflow:** A diagram showing the progression from '1 - Data Collection' to '2 - Basic Analysis, Mitigation and Submission' (which is highlighted with a red box and a red arrow pointing to it), then to '3 - Approver Review' and finally '4 - Completed'.
- Assessment Details:** Shows the assessment ID '4640\_FIREBIRD15246-PRE\_RFP-BASELINE' and the status 'Assessment Conducted'.
- Risk Tab Content:** This section is currently active. It includes tabs for 'Show Assessment/Inspection Results', 'Analysis and Mitigation' (selected), and 'Submission'. Below these tabs are buttons for 'Risk' (selected) and 'Compliance'. A message states: 'This is where you may adjust and reduce your risk by managing countermeasures. [More]'. A 'Your Risk Overview' section shows a progress bar labeled 'CURRENT Risk Level: 59.5%' with a red-to-green gradient. Buttons for 'Export to Excel', 'Upload Responses', 'Add/Edit Comment', 'Manage Countermeasure Status', 'Propose All Countermeasures', and 'Apply Countermeasure Cost' are present.
- Countermeasures Table:** A table listing various countermeasures with columns for Category, Mitigation, Status, Due Date, Comment, Cost, Risk Red./\$, and Risk Red. Wt. Some entries include:
 

Category	Mitigation	Status	Due Date	Comment	Cost	Risk Red./\$	Risk Red. Wt.
TSN - Planning (PL) - 03	The program shall ensure design specific information on external networks is encrypted.	Originally In Place				1.716%	
CUI/CTI - Media Protection (MP) - 10	The program shall implement Data at Rest (DAR) encryption on all external media.	Not Implemented				1.716%	
CPI - Media Protection (MP) - 09	The program shall implement Data at Rest (DAR) encryption on all external media.	Originally In Place				1.716%	
CLASSIFIED - Media Protection (MP) - 01	The program shall implement data at rest (DAR) encryption on all external media.	Originally In Place				1.716%	

Figure 59: Basic Analysis – Risk Tab

## Countermeasure Status

Countermeasure status is based on the answers input or uploaded in the assessment. Those answered “Yes” will show as originally in place. Those answered “No” will show as “Not Implemented”. Any countermeasure status marked “N/A” will not show in the list.

## Countermeasure Grid Labels

Countermeasures							
Category	Mitigation	Status	Due Date	Comment	Cost	Risk Red./\$	Risk Red. Wt.
CUI/CTI - Operations Security - 01	Operations Security (OPSEC) for the program IAW the OPSEC Plan and Critical Information List provided by the Government.	Originally In Place			1.728%		
CPI - Operations Security - 02	The program shall apply Operations Security (OPSEC) in their management of the Program IAW the OPSEC Plan and program's Critical Information List provided by the Program office.	Not Implemented			1.728%		
CPI - Operations Security - 01	The program shall employ OPSEC safeguards to protect Critical Information throughout the system development life cycle as documented in the OPSEC plan.	Not Implemented			1.728%		

Figure 60: Risk tab – Countermeasure Grid

Labels on the grid of countermeasures are shown in the table below:

Column Label	Description
Category	The countermeasure category of this countermeasure.
Mitigation	This is the shall statement which will be in the SOW report describing the security requirement.
Status	The current status of this countermeasure.
Due Date	When a countermeasure is assigned with a due date, the date will show here.
Comment	Comments added by user.
Cost	Based on user input, this is the cost of implementing this countermeasure. It includes actual cost, supplies and maintenance.
Risk Reduction/\$	This is a calculation of the cost of implementing the countermeasure verses the amount of risk reduced by implementing the countermeasure.
Risk Red Wt.	This is a relative number to show the risk reduced by implementing the countermeasure. Different countermeasures will have different effects on risk. The higher the number, the greater the risk will be reduced when implemented.

Figure 61: Countermeasure Grid Labels

## Risk Tab Buttons

Like other pages, the risk page buttons have the same functionality as in other pages. There are additional buttons including Manage Countermeasures, Propose all Countermeasures and Apply countermeasure Cost. The table below provides a brief description of each button and the next sections explain the new buttons in detail.



Figure 62: Risk Tab Buttons

Button	Function	Used for
<b>Export to Excel</b>	Exports the list of countermeasures and the current status into a customized Excel file.	Completing the countermeasure questions in Excel (to improve efficiency). This is also the file sent to offerors to complete as part of their RFP response.
<b>Upload Responses</b>	Uploads an updated countermeasure file.	Improving efficiency when answering countermeasures.
<b>Add/View Comment</b>	Pop up screen to add or view comment on an asset	Add or view a comment on a selected countermeasure.
<b>Manage Countermeasure Status</b>	Change the status of a countermeasure. For example, from "Not implemented" to "Proposed".	Propose, implement and/or assign a countermeasure. Only those implemented will affect risk.
<b>Propose all countermeasures</b>	Changes the status of any countermeasure Not implemented to "Proposed" or "Implemented"	Applying the same changes to all unimplemented countermeasures.
<b>Apply countermeasure Cost</b>	Allows the user to input cost associated with implementing this countermeasure	Used in trade space analysis to determine cost of security. When costs are entered, the risk reduction per \$ will populate. (This functionality not currently being used).
<b>Export to Excel</b>	Exports the list of countermeasures and the current status into a customized Excel file.	Completing the countermeasure questions in Excel (to improve efficiency). This is also a file which can be sent to offerors to update their countermeasure status as part of their RFP response.
<b>Upload Responses</b>	Uploads an updated countermeasure file.	Improving efficiency when answering and updating countermeasures.

Figure 63: Risk Button Definitions 1

## Manage Countermeasure Status

Countermeasures not in place can be updated to be proposed or implemented. They can also be assigned with a due date to someone else within the organization.

To change the status of the countermeasure, first select the countermeasure to be changed. Then click on Manage Countermeasure Status button. This will result in a pop up window where you can make the change(s). Click on Save to save your changes. The risk bar change as you change countermeasure status.

The screenshot shows a software interface for managing countermeasure status. At the top, there is a progress bar labeled "CURRENT Risk Level: 16.3%" with a green section on the left and a red section on the right. Below the bar are several buttons: "Export to Excel", "Upload Responses", "Add/Edit Comment", "Manage Countermeasure Status" (which is highlighted with a red box), and "Propose All Countermeasures". There is also a button "Apply Countermeasure Cost".

The main area displays a table titled "Countermeasures" with columns: Category, Mitigation, Status, Due Date, Comment, Cost, Risk Red./t, and Risk Red. Wt. A specific row is selected, highlighted with a yellow background and a red dashed border. This row corresponds to the countermeasure "CPI - Operations Security - 02". The mitigation details for this row are:

**CPI - Operations Security - 02**  
 The program shall apply Operations Security (OPSEC) in their management of the Program IAW the OPSEC Plan and program's Critical Information List provided by the Program office.

The "Status" column for this row shows "Not Implemented".

A modal dialog box titled "Manage Countermeasure Status" is open over the table. It contains the following fields:

- Countermeasure:** The program shall apply Operations Security (OPSEC) in their management of the Program IAW the OPSEC Plan and program's Critical Information List provided by the Program office.
- Status Options:**
  - Mark as unproposed.
  - Mark as proposed without assigning.
  - Mark as proposed and assign to an EPRM user.
  - Mark as proposed and assign to external personnel.
- Due Date:** To be completed on  [Clear Due Date](#)
- Implementation Status:**
  - Mark as implemented.
  - Implementation Date:** Implemented on  [Clear Implementation Date](#)
- Buttons:** [Save](#) [Cancel](#)

Figure 64: Managing Countermeasure Status

## Countermeasure Status Changes

The following table provides a description of each of the Manage Countermeasure status choices.

Selection	Function	Use When
<b>Mark as unproposed</b>	Changes a previously proposed countermeasure to unproposed and increases planned risk in the risk bar graph.	When making changes to proposed countermeasure.
<b>Mark as Proposed without assigning</b>	Changes countermeasure status to Proposed and reduces planned risk in the risk bar graph. <b>No due date is required.</b>	When proposing a countermeasure but unsure of who it will be assigned to. You can update the countermeasure and assign it later.
<b>Mark as Proposed and assign to an EPRM user</b>	Changes countermeasure status to Proposed and reduces planned risk in the risk bar graph. A drop down of EPRM users allows you to select the assignee.	When proposing a countermeasure and assigning it to an EPRM user. The assignee will receive an email indicating they have been assigned a countermeasure to implement.
<b>Mark as Proposed and assign to external personnel</b>	Changes countermeasure status to Proposed and reduces planned risk in the risk bar graph. A text field for adding an email allows you to select the assignee. Assigner must update countermeasure once implemented since assignee does not have access.	When proposing a countermeasure and assigning it to a non - EPRM user. The assignee will receive an email indicating they have been assigned a countermeasure to implement.
<b>To be completed on</b>	When assigning a proposed countermeasure to someone, adds a date the countermeasure should be implemented.	When adding a deadline to when the countermeasure should be implemented.
<b>Mark as Implemented</b>	Changes countermeasure status to Implemented and is reflected in current risk in the risk bar graph.	When a countermeasure has been fully implemented.
<b>Implemented on</b>	Adds the date the countermeasure was implemented.	Adding the date the countermeasure was implemented.

Figure 65: Managing Countermeasure Status Definitions

## Propose All Countermeasures

Pressing this button will change anything not implemented to Proposed. It will show as yellow on the bar graph as “Planned Risk”. It does not affect actual risk. i.e., a user cannot mark everything proposed to get a risk score reduced. Only *implementing* the countermeasure changes risk.

## Use Export/Upload Functionality to Update Countermeasures

If you are making a lot of changes or need an update from the Prime or Subs, you can use the Export to Excel and Upload Responses functionality. Export to Excel creates a file which can be updated then uploaded.

Only countermeasures *not implemented* or *proposed* can be updated. Those marked “In place” cannot change. In addition, you cannot assign countermeasures. Assignment is done using the Manage Countermeasures button.

The screenshot shows a Microsoft Excel spreadsheet titled "Analysis and Mitigation Export (1).xlsx - Excel". The spreadsheet contains a table named "Countermeasures" with columns: Category, Mitigation, Status, Due Date, Comment, Cost, Risk Red./!, and Risk Red. Wt. A red box highlights the top row of buttons: "Export to Excel", "Upload Responses", "Add/Edit Comment", "Manage Countermeasure Status", and "Propose All Countermeasures". Below these buttons is a "Countermeasures" table. A red arrow points from the "Propose All Countermeasures" button down to the "Countermeasure Status" dropdown menu in column E, row 25. The dropdown menu shows three options: "Not Implemented", "Proposed", and "Implemented". The "Not Implemented" option is selected. The "Proposed" and "Implemented" options are grayed out. The "Countermeasure Status" dropdown menu is also highlighted with a red box.

Category	Mitigation	Status	Due Date	Comment	Cost	Risk Red./!	Risk Red. Wt.

Figure 66: Managing Countermeasure Status with Excel

## Reading the Risk Bar Graph

As the status of countermeasures are changed, the risk bar graph will reflect changes. The most up to date risk bar graph of an assessment will show in reports.

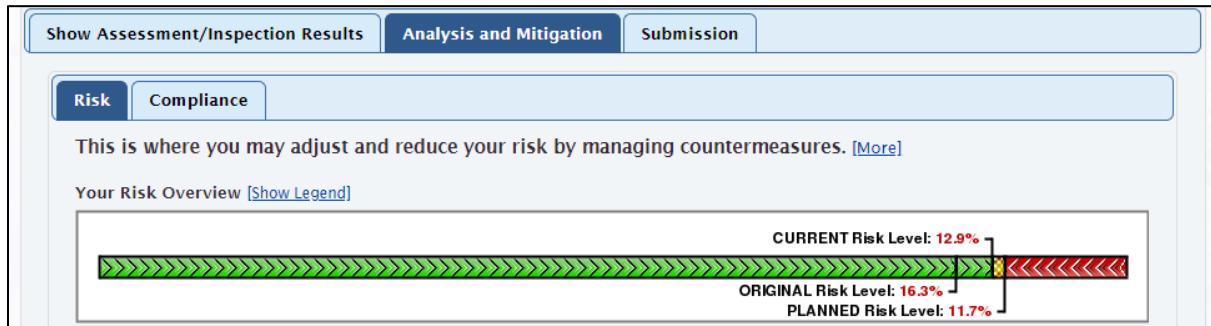


Figure 67: Risk bar showing updated countermeasure status

Label	Description	As a Result of
<b>Original Risk (green)</b>	Risk at the time the assessment was completed and locked. The lower the number the less the risk.	Answers provided in assessment.
<b>Planned Risk (yellow)</b>	What risk <u>would be</u> if the countermeasures proposed are implemented.	Proposing countermeasures.
<b>Current Risk (green)</b>	Current risk.	Implementing countermeasures.

Figure 68: Risk Bar Label Definitions

## Compliance Tab

The compliance tab shows the percent of countermeasures implemented versus the total number of countermeasures. It also shows how countermeasures link with specific sources.

Countermeasures can be updated on this tab or the Risk tab. The buttons with the same name function the same. (See page 46).

An additional feature on the compliance tab is the ability to filter by specific reference to see the status of each countermeasure relative to the source(s) driving it. For example, if you wanted to see your compliance with DoD 5200.22, you could filter for the reference NIST and see the status of the countermeasures relative to 5200.22. The figure on the following page shows the steps.

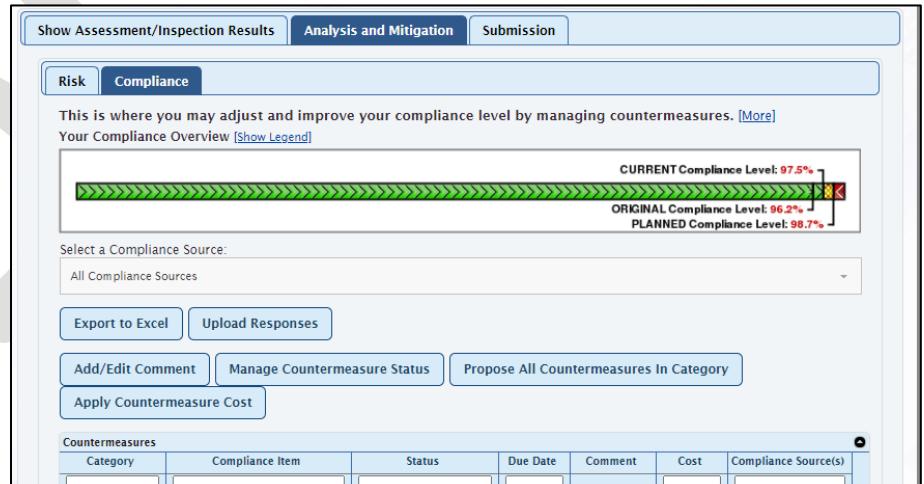


Figure 69: Compliance Tab

This is where you may adjust and improve your compliance level by managing countermeasures. [More]

**Compliance with a specific reference shows here.**

CURRENT Compliance Level: 50% PLANNED Compliance Level: 100%

Select a Compliance Source:

DoDI 5200.02, 21 March 2014

Use the drop down to select a specific reference

Export to Excel Upload Responses

Add/Edit Comment Manage Countermeasure Status Propose All Countermeasures In Category

Apply Countermeasure Cost

Countermeasures

Category	Compliance Item	Status	Due Date	Comment	Cost	Compliance Source(s)
CUI/CTI - Planning (PL) - 04.k	Personnel with access to classified information shall be under a continuous monitoring program.	Originally In PI				DoDI 5200.02, 21 March 2014, NIST SP 800-53 Rev. 4, Apr 2013, incl updates as of 22 Jan 2015, NIST SP 800-53A Rev. 4, 18 Dec 2014
CLASSIFIED - Program Management (PM) - 03	Personnel with access to classified design, manufacturing, or assembly information shall be under the DoD Continuous Monitoring program.	Proposed 2020-09-24				DoDI 5200.02, 21 March 2014, NIST SP 800-53 Rev. 4, Apr 2013, incl updates as of 22 Jan 2015, NIST SP 800-53A Rev. 4, 18 Dec 2014

**Reference for the countermeasure compliance**

Figure 70: Compliance Tab – compliance with a specific reference

## Submission Tab

The submission tab allows a user to submit their assessment to the next level up in the hierarchy. This is an optional step. Once submitted, supervisors can pass an assessment and/or ask for a re-assessment with a specific date. Assessment and Inspection results show in the Show Assessment/Inspection Results tab.

Show Assessment/Inspection Results Analysis and Mitigation **Submission**

**Assessment/Inspection Results**

Please answer the following questions about the assessment/inspection to final

An \* denotes the field is required

Is the assessed/inspected node adequate to pass assessment/inspection? \*

Does the assessed/inspected node require a reassessment/reinspection?

To be completed by

Comments (required for not adequate assessment/inspection)

**Once submitted, approvers can mark as Adequate or Not Adequate and suggest a re-assessment date. (This is an optional step).**

**Submit**

**Confirm**

\*WARNING: This step in the process is optional. If you choose to proceed, your assessment will be sent to the next manager(s) up in your hierarchy and you will no longer be able to edit your assessment. Prior to submitting, confirm with your designated approver that he/she has an existing EPRM account.

Do you want to continue?\*

Yes No

Figure 71: Submitting an assessment.

## 4 Program Protection Plan

Program Protection Plan tracking is automated in ASM. Plan can be created as part of the PMO assessment process or created directly then associated with an assessment.

### Create a PPP Outside of an Assessment

You can create a PPP directly through Manage Survey Responses then later associate it with an assessment. Once the PPP is created, it can be associated with an assessment by clicking on the Program Protection Plan button in an assessment and selectin Associate an Existing PPP.

The screenshot displays the EPRM Acquisition Security interface. At the top, there is a welcome message and a main menu with several icons: Main Menu, Manage Assessments, Advanced Analysis, Manage Survey Responses (which is highlighted with a red box), and User Guides and References. A callout box points to the Manage Survey Responses icon with the text "PPP can also be created directly through Manage Survey Responses". Below the menu, there is a section for managing surveys, featuring a large green "START" button and a table titled "Started and Completed Surveys". The table shows one row: id 3203, Survey Name PPP - 123456 - PMO, Due Date (empty), Status Locked, Owner David Smith, Node AFLCMC/Armament (EB) > FIREBIRD, Created 09/25/2020, and Objective(s) Program Protection Plan (PPP). A red arrow points from the "Manage Survey Responses" icon in the main menu down to the "START" button. In the bottom portion of the interface, there is a form for creating a new survey. One question asks "Does your program have a Program Protection Plan?" with a dropdown menu showing "No". Another question asks "If you are a PMO, please complete a PPP." with a checkbox labeled "Program Protection Plan" which is checked. A third question asks "What ACAT level is this program?" with a dropdown menu showing "ACAT II". A fourth question asks "If other, please describe:" with a text input field. The "OPERATIONS & SUSTAINMENT" section includes a question "Is the program..." with a dropdown menu showing "Yes". A modal dialog box titled "Associate Program Protection Plan" is open, asking "Would you like to:" with two options: "Create and associate a new Program Protection Plan" (radio button selected) and "Associate an existing Program Protection Plan". A red box highlights the "Create and associate a new Program Protection Plan" option.

Figure 72: Directly Create a Survey

## Update the PPP

The PPP can be updated as often as needed as requirements are met. While you can navigate back and forth from the PPP to the assessment, to update it you would use Manage Survey Responses. (This is being changed in future versions).

\*\*\*UPDATE COMING SOON!\*\*\* Users will be able to update the PPP from the assessment.

Welcome to EPRM  
**Acquisition Security**

This is your resource to complete the Risk Assessment process. EPRM will help you understand risk analysis by assisting you in identifying your assets and what it can do better. You can assign tasks and create reports to truly understand and explain your Risk.

**Click on Manage Survey Responses**

Main Menu      Manage Assessments      Advanced Analysis      **Manage Survey Responses**      User Guides and References

Enable Accessibility

[Home](#) > Manage Surveys Home

This is where you may create a new survey or view / modify existing surveys based on privileges or permissions unique to your User Profile. [\[More\]](#)

**Locate and select the previously created survey in the list at the bottom of the screen. Double click to open.**

**Start a New Survey**

Started and Completed Surveys - To open, double-click on a row or select a row and click on open button at the bottom of the grid.							
id	Survey Name	Due Date	Status	Owner	Node	Created	Objective(s)
3203	PPP - 123456 - PMO		Locked	David Smith	AFLCMC/Armament (ES) > FIREBIRD	09/25/2020	Program Protection Plan (PPP)
3205	PPP New Created directly		Locked	David Smith	USAF Acquisition Security > AFNWC	09/25/2020	Program Protection Plan (PPP)
3202	ASM-20200924 - 123456 - PPP		1 - Data Collection	Cathy Sumeracki	AFLCMC/Armament (ES) > FIREBIRD	09/24/2020	Program Protection Plan (PPP)
3199	100002020_Training_FPP		Locked	Cathy Sumeracki	USAF Acquisition Security > Air	09/10/2020	Program Protection Plan (PPP)

Figure 73: Update a Survey

Once the PPP is opened, Click on **Open for Editing** to update.

This is your survey process. We'll guide you through it step by step.  
Use the links below to guide you through the steps to understand your security posture and your next steps to reduce your vulnerability and risk.

**Until the PPP is opened for editing, it will show as read only. Click on Open for Editing to unlock and make updates.**

3203\_PPP - 123456 - PMO  
Survey of FIREBIRD, 09/25/2020 (Locked)  
Conducted by David Smith with objectives: Program Protection Plan (PPP)

**Survey Administration**

- [Navigate to Assessment](#) Navigate back to assessment
- Open for Editing** *Unlock this survey for editing*
- [Rename](#) Change the name of this survey
- [Share this Survey](#) Share this survey with other users
- [Change Owner](#) Give responsibility for this survey to another user
- [Delete](#) Permanently delete this survey
- [File/Image Upload](#) Upload files or images

**Survey Workflow**

Home > Manage Surveys Home > 3203\_PPP - 123456 - PMO

This is your survey process. We'll guide you through it step by step.  
Use the links below to guide you through the steps to understand your security posture and your next steps to reduce your vulnerability and risk.

**PPP is no longer read only. Click on Data Collection.**

1 - Data Collection CLICK HERE

3203\_PPP - 123456 - PMO  
Survey of FIREBIRD, 09/25/2020 (Locked)  
Conducted by David Smith with objectives: Program Protection Plan (PPP)

Home > Manage Surveys Home > 3203\_PPP - 123456 - PMO > 1 - Data Collection

This will set-up your 1 - Data Collection.  
Use the links below to guide you through the steps.

**Click on Page 1 to open PPP for editing.**

CLICK HERE Page 1 FINISH AND LOCK CLICK HERE

[Back to Survey Home Page](#)

Figure 74: Update a Survey

Once the PPP is open, **make edits and Click Continue**.

**Questions**  
Please answer the following questions.

**Make edits to the PPP.**

**Program Protection Plan (PPP)**

1. Has a PPP been developed and approved for ALL programs beginning at MS A and every subsequent Milestone Decision including Full-Rate Production, and approved by the MDA?  Yes

PPP Date Approved:   
PPP Date Due

PPP Required Documentation submitted?\*  Yes

PPP Remarks:  
Program Plan is in draft; awaiting adjudication from WG and others.

1.a. Have system modifications or upgrades been addressed in the PPP? For legacy systems, PPP requirements for modifications can be satisfied by updating or annexing an existing PPP, creating a separate PPP for each modification, or creating a new PPP for the entire weapon system addressing all modification protection measures. (Note: The annex is effectively a "stand alone" PPP for the modification/upgrade effort.)  -Select-

System Modification Remarks:

**Click Continue**

**Back** **Navigate to Assessment** **Exit to Data Collection/Lock** **Continue**

Home > Manage Surveys Home > 3203 PPP - 123456 - PMO > 1 - Data Collection

This will set-up your 1 - Data Collection.  
Use the links below to guide you through the steps.

  **Remember to Finish and Lock**

[Page 1](#)

**Back to Survey Home Page**

Figure 75: Update a Survey

## When completing the Program Protection Plan:

- **Answer every question.** (You will be unable to finish and lock without completing).
- **Always Finish and Lock** the plan (this ensures the data will be included in reports).
- **Create** the plan through **the PMO assessment**.
- **Update** the plan through **Manage Survey Responses** (this is being updated to be able to edit from the assessment).

## Other PPP Functions

In addition to navigating back and forth between the PPP and the associated assessment, other functions on the Survey Home screen are shown below.

Button	Function	Used for
<b>Navigate to Assessment</b>	Navigate back to assessment	To return to assessment so you can update both more efficiently
<b>Open for Editing</b>	Unlock this survey for editing	Updating the PPP
<b>Rename</b>	Change the name of this survey	Program name change or error in name
<b>Share this Survey</b>	Share this survey with other users	Share with a supervisor or other ASM user for review
<b>Change Owner</b>	Give responsibility for this survey to another user	When program responsibility changes
<b>Delete Permanently</b>	Delete this survey	Uncorrectable errors in a PPP or when a new PPP is requested
<b>File/Image Upload</b>	Upload files or images	When required documentation is required
<b>Export to Excel</b>	Export to Excel for Offline Processing	Complete the questions in Excel and upload to ASM for more efficiency or when multiple people need to provide input.
<b>Upload Responses</b>	Upload Responses from Excel	Adding the completed PPP information into ASM more efficiently.
<b>Reports</b>	Generate reports and survey aids	Run reports (No reports available at this time).
<b>View POCs</b>	View points of contact	Request for POC on a program

Figure 76: Other Survey Functions

## 5 Reports

ASM has several reports. Reports fall into two categories:

- 1) Single assessment reports and
- 2) Multiple assessment reports

Each type of report is accessed through two different processes. Single assessment reports are accessed through the Assessment main menu. Multiple assessment reports are accessed through Advanced Analysis. You can use Advanced Analysis for detail on a single assessment.

### Single Assessment Reports

Single assessment reports can be found on the Assessment Home Page. You must be in the assessment to access the report. After logging in, click on Manage Assessments and locate the assessment you would like to run a report on. Once on the main menu of the Assessment, click on the Reports button.

### Multiple Assessment Reports

Multiple assessment Reports are access through the Advanced Analysis icon. Here you can select multiple assessments to include in a report. Reports generated using Advanced Analysis are aggregate of all assessments selected. More on Advanced Analysis can be found in Section XX.

### Recommended Reports for ASM

Two key reports for ASM include:

- 1) Executive Summary Report (single assessment report)
- 2) Dashboard Report (Single or multi-assessment report)

These reports were specifically designed for the Acquisition community.

#### Executive Summary Report

The Executive Summary Report provides a high-level view of the risk for an organization. It includes overall risk, assets, threat changes and the countermeasure implemented. It also provides the status of the Program Protection Plan.

<b>ASM - Program Protection Planning Executive Summary</b>  Program Name:  ACAT Level: ACAT IC  Assessment Name: ASM-20201005-Firebird-PM Approved RFP-No CAGE code- Program Office
--

Figure 77 Executive Summary Report title page.

## Dashboard Report

The Dashboard report is accessed through Advanced Analysis and can be generated with information based on multiple assessments. This is an at-a-glance report showing risk, planned risk and status of the Program Protection plan.

It is created in Excel but can easily be cut and pasted into a PowerPoint presentation.

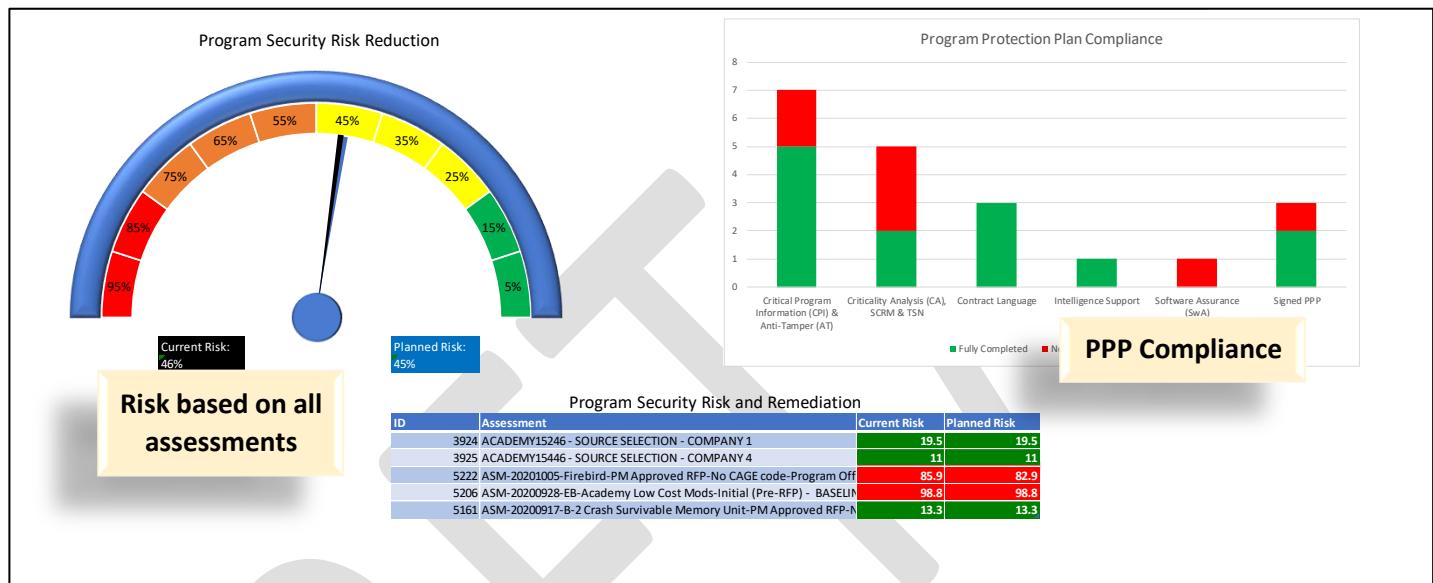


Figure 78: Dashboard Report

## 6 Advanced Analysis

Advanced Analysis allows for the creation of reports with multiple assessments. This is the report used when reviewing multiple responses from offerors during the RFP process.

Analysis can be based on any of the profile questions or assets in programs. For example, a risk comparison of different programs at the same ACAT level or with the same assets.

Figure 79: Advanced Analysis- Filtering for specific assessments

The following shows the steps in using Advanced Analysis to compare Offerors in the RFP process. In this example, we are filtering for Source Selection assessments for contract 123456.

First filter by the profile question by clicking on the arrow to the left of Select Profile questions for Analysis. The system will ask you to add an objective. (Note: Only those objectives you have access to will show. Select Add then select Acquisition Security.

Figure 80: Advanced Analysis - Select Acquisition Security Objective

Next, locate the Contract Number and select. This will result in a pop up window asking for the contract number. Enter the contract number. Remember to click on Save Profile Questions Filter to save your selections.

Add Profile Question Filter

- Marine Systems (IBTL)
- Materials Raw & Processed (IBTL)
- Medical Technology (IBTL)
- Navigation Systems (HPG)
- Nuclear Information or Technology (IBTL)
- Optics (IBTL)
- Positioning, Navigation, and Time (IBTL)
- Radars (HPG)
- Radars (IBTL)
- Restricted Counter Low Observables (CLO) Systems and Technologies (LO and CLO)
- Restricted Low Observables (LO) Technologies (LO and CLO)
- Sensors (Acoustic) (IBTL)
- Signature Control (IBTL)
- Software (IBTL)
- Space Systems (IBTL)
- System Management (HPG)
- Tier 1 Technology (Tier 1)
- Tier 2 Technology (Tier 2)
- Weapons (HPC)

Contract Number

Cage Code

Location

Is this the Prime?

Add Profile Question Filter

Selected Objective: Acquisition Security

Selected Question: Contract Number

Selected Responses: 123456

Contract Number 123456

Save Profile Question Filter

Figure 81: Advanced Analysis – Filtering for Contract Number

The next screen will show you the filters selected. Here the system will look in the Acquisition Security objective (ASM) for all assessments which contain the contract number 123456. To confirm this filter, click on Apply Profile Questions Filter button located at the bottom right. You could also adjust your filters (add, edit and/or delete) by using the buttons above the filter.

Select Profile Questions for Analysis ----- FILTER STATUS: Not Applied								
Add	Edit	Delete						
<b>Profile Question Filters</b> <table border="1"> <thead> <tr> <th>Objective</th> <th>Question</th> <th>Responses</th> </tr> </thead> <tbody> <tr> <td>Acquisition Security</td> <td>Contract Number</td> <td>123456</td> </tr> </tbody> </table>			Objective	Question	Responses	Acquisition Security	Contract Number	123456
Objective	Question	Responses						
Acquisition Security	Contract Number	123456						
Page 1 of 1   50   Rows 1 - 1 of 1 Clear Profile Questions Filter <b>Apply Profile Questions Filter</b>								

Figure 82: adding a Profile Question Filter

Assessments matching this filter will show in the bottom grid. You can continue with selected assessments or further filter using the filter boxes above each column. In this example, we added the filter “Source” to keep the comparison to Source Selection assessments.

Keep the checkbox marked to include in the analysis. Remove the checkmark if you do not want the assessment included.

Completed Assessments										<a href="#">Print</a>
<input type="checkbox"/>	ID	Assessment	Status	Objective(s)	Start Date	Updated By	Last Updated	Node	Account	<a href="#">Edit</a>
<input type="checkbox"/>		Source								
<input checked="" type="checkbox"/>	5177	ASM-20200804 -Firebird-Source Selection -58746	2 – Basic Analysis, Mitigation and Submission	Acquisition Security	09/22/2020	Cathy Sumeracki	09/24/2020	AFLCMC/Armar (EB) > FIREBIRD	Acquisition Security	
<input checked="" type="checkbox"/>	5020	ASM-20200804 -Firebird-Source Selection -87451	2 – Basic Analysis, Mitigation and Submission	Acquisition Security	08/04/2020	Joseph Banks	08/04/2020	AFLCMC/ISR & SOF (WI) > WII	Acquisition Security	
<input checked="" type="checkbox"/>	5035	ASM-20200804 -Firebird-Source Selection -22231	2 – Basic Analysis, Mitigation and Submission	Acquisition Security	08/04/2020	Terry Alphin	08/04/2020	USAF Acquisition Security > AFRL	Acquisition Security	

Figure 83: Advanced Analysis - Selection of Filtered Assessments



The risk bar below indicates original, current and planned risk level(s) for the selected assessment(s). (NOTE: if no mitigating actions have been applied, no current or planned risk will display)

The total 100% value of the bar represents the total overall risk possible for the selected assessment(s) and the values displayed are the average value for all of the selected individual risk assessment(s). Click "Show Legend" for more information on labels and color coding. Also, note that this page is for data display only, users cannot plan or make changes here; those actions are performed in Basic Analysis and Mitigation.

Your Risk Overview [\[Show Legend\]](#)

**CURRENT Risk Level: 43%**



ORIGINAL Risk Level: 44.2%      PLANNED Risk Level: 39.3%

Assets	Threats	Vulnerabilities	Countermeasures	Risk Scenarios	Reports	Dashboard

**Risk by Assessment (3 assessments)**

ID	Assessment	Current Risk Score	Planned Risk Score
5177	ASM-20200804 -Firebird-Source Selection - 58746	12.9	11.7
5035	ASM-20200804 -Firebird-Source Selection - 87451	18.5	13.9
5020	ASM-20200804 -Firebird-Source Selection - 22231	97.8	92.2

Figure 84: Advanced Analysis – Comparison of Offerors for Contract 123456

When using Advanced Analysis, the buttons on the left side of the screen are relative to the assessments in the list on the right. In the example below, it would be for three assessments. Reports generated from this page reflect the risk for the total of all assessments in the list.

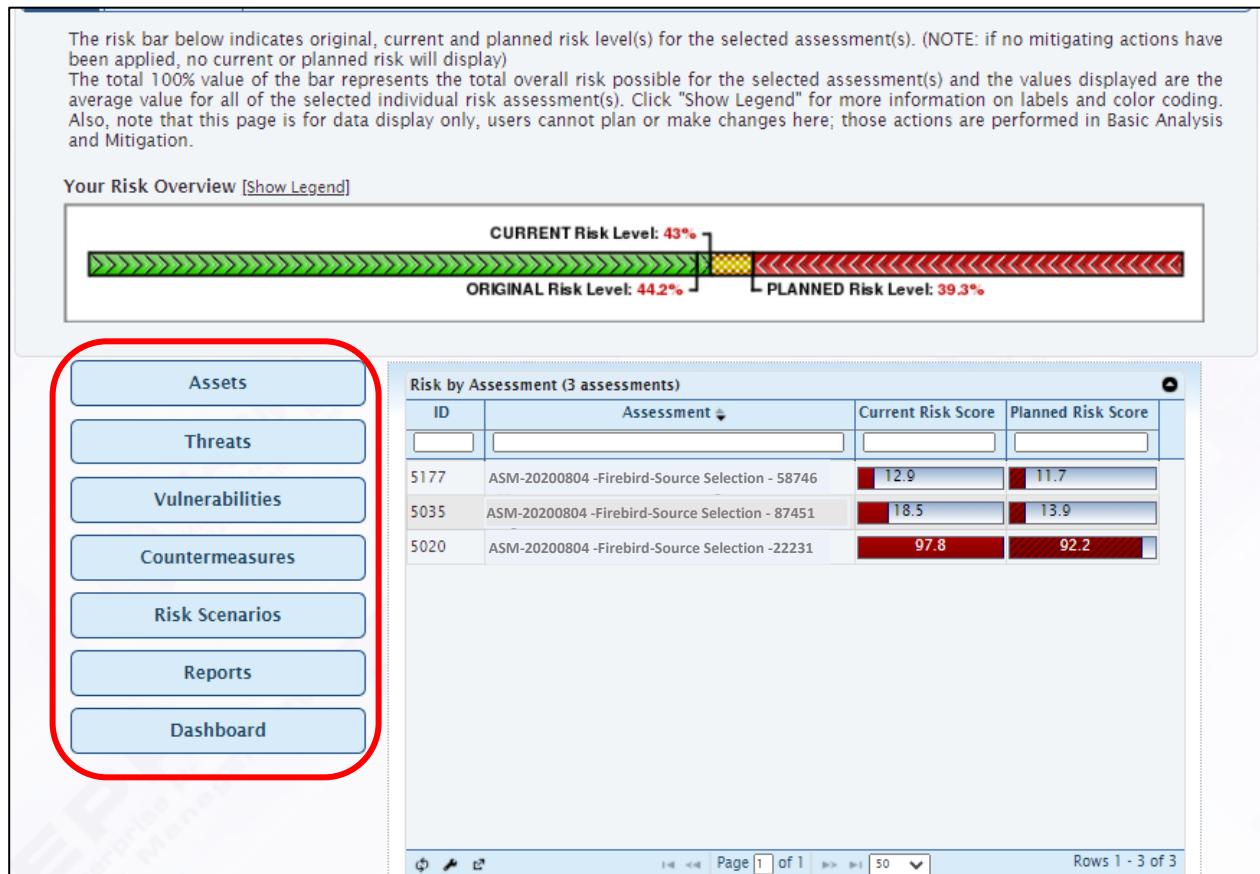
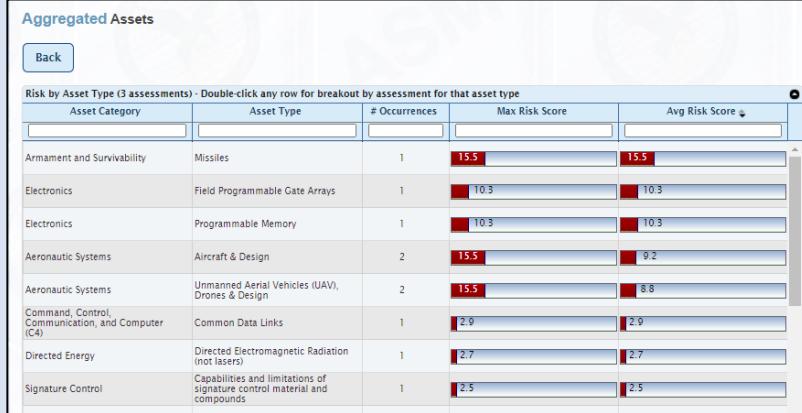
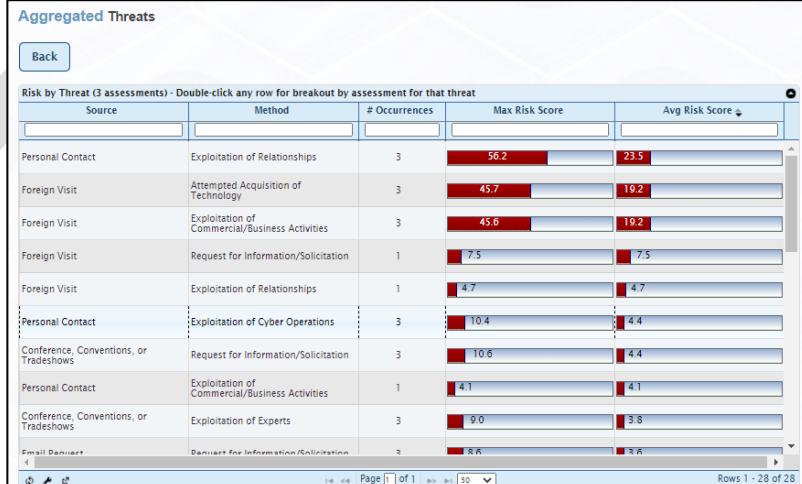
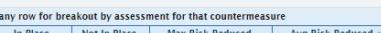


Figure 85: Reports available in Advanced Analysis.

## Advanced Analysis – Sample Reports

In addition to the screen comparison, Advanced Analysis has several reports based on the aggregate of all selected assessments. The table below provides a brief over of the report.

Button	Description	Used For	Example																																																							
Assets	Creates aggregate list of all assets, number of occurrences and their associated risk scores	Determining the assets most at risk	 <p><b>Aggregated Assets</b></p> <p>Risk by Asset Type (3 assessments) - Double-click any row for breakout by assessment for that asset type</p> <table border="1"> <thead> <tr> <th>Asset Category</th> <th>Asset Type</th> <th># Occurrences</th> <th>Max Risk Score</th> <th>Avg Risk Score</th> </tr> </thead> <tbody> <tr> <td>Armament and Survivability</td> <td>Missiles</td> <td>1</td> <td>15.5</td> <td>15.5</td> </tr> <tr> <td>Electronics</td> <td>Field Programmable Gate Arrays</td> <td>1</td> <td>10.3</td> <td>10.3</td> </tr> <tr> <td>Electronics</td> <td>Programmable Memory</td> <td>1</td> <td>10.3</td> <td>10.3</td> </tr> <tr> <td>Aeronautic Systems</td> <td>Aircraft &amp; Design</td> <td>2</td> <td>15.5</td> <td>9.2</td> </tr> <tr> <td>Aeronautic Systems</td> <td>Unmanned Aerial Vehicles (UAV), Drones &amp; Design</td> <td>2</td> <td>15.5</td> <td>8.8</td> </tr> <tr> <td>Command, Control, Communication, and Computer (C4)</td> <td>Common Data Links</td> <td>1</td> <td>2.9</td> <td>2.9</td> </tr> <tr> <td>Directed Energy</td> <td>Directed Electromagnetic Radiation (not lasers)</td> <td>1</td> <td>2.7</td> <td>2.7</td> </tr> <tr> <td>Signature Control</td> <td>Capabilities and limitations of signature control material and compounds</td> <td>1</td> <td>2.5</td> <td>2.5</td> </tr> </tbody> </table>	Asset Category	Asset Type	# Occurrences	Max Risk Score	Avg Risk Score	Armament and Survivability	Missiles	1	15.5	15.5	Electronics	Field Programmable Gate Arrays	1	10.3	10.3	Electronics	Programmable Memory	1	10.3	10.3	Aeronautic Systems	Aircraft & Design	2	15.5	9.2	Aeronautic Systems	Unmanned Aerial Vehicles (UAV), Drones & Design	2	15.5	8.8	Command, Control, Communication, and Computer (C4)	Common Data Links	1	2.9	2.9	Directed Energy	Directed Electromagnetic Radiation (not lasers)	1	2.7	2.7	Signature Control	Capabilities and limitations of signature control material and compounds	1	2.5	2.5										
Asset Category	Asset Type	# Occurrences	Max Risk Score	Avg Risk Score																																																						
Armament and Survivability	Missiles	1	15.5	15.5																																																						
Electronics	Field Programmable Gate Arrays	1	10.3	10.3																																																						
Electronics	Programmable Memory	1	10.3	10.3																																																						
Aeronautic Systems	Aircraft & Design	2	15.5	9.2																																																						
Aeronautic Systems	Unmanned Aerial Vehicles (UAV), Drones & Design	2	15.5	8.8																																																						
Command, Control, Communication, and Computer (C4)	Common Data Links	1	2.9	2.9																																																						
Directed Energy	Directed Electromagnetic Radiation (not lasers)	1	2.7	2.7																																																						
Signature Control	Capabilities and limitations of signature control material and compounds	1	2.5	2.5																																																						
Threats	Creates aggregate list of all threats, number of occurrences and their associated risk scores	Determining the highest threats	 <p><b>Aggregated Threats</b></p> <p>Risk by Threat (3 assessments) - Double-click any row for breakout by assessment for that threat</p> <table border="1"> <thead> <tr> <th>Source</th> <th>Method</th> <th># Occurrences</th> <th>Max Risk Score</th> <th>Avg Risk Score</th> </tr> </thead> <tbody> <tr> <td>Personal Contact</td> <td>Exploitation of Relationships</td> <td>3</td> <td>56.2</td> <td>23.5</td> </tr> <tr> <td>Foreign Visit</td> <td>Attempted Acquisition of Technology</td> <td>3</td> <td>45.7</td> <td>19.2</td> </tr> <tr> <td>Foreign Visit</td> <td>Exploitation of Commercial/Business Activities</td> <td>3</td> <td>45.6</td> <td>19.2</td> </tr> <tr> <td>Foreign Visit</td> <td>Request for Information/Solicitation</td> <td>1</td> <td>7.5</td> <td>7.5</td> </tr> <tr> <td>Foreign Visit</td> <td>Exploitation of Relationships</td> <td>1</td> <td>4.7</td> <td>4.7</td> </tr> <tr> <td>Personal Contact</td> <td>Exploitation of Cyber Operations</td> <td>3</td> <td>10.4</td> <td>4.4</td> </tr> <tr> <td>Conference, Conventions, or Tradeshows</td> <td>Request for Information/Solicitation</td> <td>3</td> <td>10.6</td> <td>4.4</td> </tr> <tr> <td>Personal Contact</td> <td>Exploitation of Commercial/Business Activities</td> <td>1</td> <td>4.1</td> <td>4.1</td> </tr> <tr> <td>Conference, Conventions, or Tradeshows</td> <td>Exploitation of Experts</td> <td>3</td> <td>9.0</td> <td>3.8</td> </tr> <tr> <td>Overall Summary</td> <td>Demands for Information/Communication</td> <td>2</td> <td>8.8</td> <td>4.4</td> </tr> </tbody> </table> <p>Page 1 of 1 Rows 1 - 28 of 28</p>	Source	Method	# Occurrences	Max Risk Score	Avg Risk Score	Personal Contact	Exploitation of Relationships	3	56.2	23.5	Foreign Visit	Attempted Acquisition of Technology	3	45.7	19.2	Foreign Visit	Exploitation of Commercial/Business Activities	3	45.6	19.2	Foreign Visit	Request for Information/Solicitation	1	7.5	7.5	Foreign Visit	Exploitation of Relationships	1	4.7	4.7	Personal Contact	Exploitation of Cyber Operations	3	10.4	4.4	Conference, Conventions, or Tradeshows	Request for Information/Solicitation	3	10.6	4.4	Personal Contact	Exploitation of Commercial/Business Activities	1	4.1	4.1	Conference, Conventions, or Tradeshows	Exploitation of Experts	3	9.0	3.8	Overall Summary	Demands for Information/Communication	2	8.8	4.4
Source	Method	# Occurrences	Max Risk Score	Avg Risk Score																																																						
Personal Contact	Exploitation of Relationships	3	56.2	23.5																																																						
Foreign Visit	Attempted Acquisition of Technology	3	45.7	19.2																																																						
Foreign Visit	Exploitation of Commercial/Business Activities	3	45.6	19.2																																																						
Foreign Visit	Request for Information/Solicitation	1	7.5	7.5																																																						
Foreign Visit	Exploitation of Relationships	1	4.7	4.7																																																						
Personal Contact	Exploitation of Cyber Operations	3	10.4	4.4																																																						
Conference, Conventions, or Tradeshows	Request for Information/Solicitation	3	10.6	4.4																																																						
Personal Contact	Exploitation of Commercial/Business Activities	1	4.1	4.1																																																						
Conference, Conventions, or Tradeshows	Exploitation of Experts	3	9.0	3.8																																																						
Overall Summary	Demands for Information/Communication	2	8.8	4.4																																																						

Button	Description	Use For	Example																																				
Vulnerabilities	Creates aggregate list of all vulnerabilities, number of occurrences and their associated risk scores	Determining the highest vulnerabilities	<p><b>Aggregated Vulnerabilities</b></p> <p>Back</p> <p>Risk by Vulnerability (3 assessments) - Double-click any row for breakout by assessment for that vulnerability</p> <table border="1"> <thead> <tr> <th>Vulnerability</th> <th># Occurrences</th> <th>Max Risk Score</th> <th>Avg Risk Score</th> </tr> </thead> <tbody> <tr><td>Vulnerability to Exploitation of Relationships via Personal Contact</td><td>3</td><td>56.2</td><td>23.5</td></tr> <tr><td>Vulnerability to Attempted Acquisition of Technology via Foreign Visit</td><td>3</td><td>45.7</td><td>19.2</td></tr> <tr><td>Vulnerability to Exploitation of Commercial/Business Activities via Foreign Visit</td><td>3</td><td>45.8</td><td>19.2</td></tr> <tr><td>Vulnerability to Request for Information/Solicitation via Foreign Visit</td><td>1</td><td>7.5</td><td>7.5</td></tr> <tr><td>Vulnerability to Exploitation of Relationships via Foreign Visit</td><td>1</td><td>4.7</td><td>4.7</td></tr> <tr><td>Vulnerability to Request for Information/Solicitation via Conference, Conventions, or TradeShows</td><td>3</td><td>10.6</td><td>4.4</td></tr> <tr><td>Vulnerability to Exploitation of Cyber Operations via Personal Contact</td><td>3</td><td>10.4</td><td>4.4</td></tr> <tr><td>Vulnerability to Exploitation of</td><td></td><td></td><td></td></tr> </tbody> </table>	Vulnerability	# Occurrences	Max Risk Score	Avg Risk Score	Vulnerability to Exploitation of Relationships via Personal Contact	3	56.2	23.5	Vulnerability to Attempted Acquisition of Technology via Foreign Visit	3	45.7	19.2	Vulnerability to Exploitation of Commercial/Business Activities via Foreign Visit	3	45.8	19.2	Vulnerability to Request for Information/Solicitation via Foreign Visit	1	7.5	7.5	Vulnerability to Exploitation of Relationships via Foreign Visit	1	4.7	4.7	Vulnerability to Request for Information/Solicitation via Conference, Conventions, or TradeShows	3	10.6	4.4	Vulnerability to Exploitation of Cyber Operations via Personal Contact	3	10.4	4.4	Vulnerability to Exploitation of			
Vulnerability	# Occurrences	Max Risk Score	Avg Risk Score																																				
Vulnerability to Exploitation of Relationships via Personal Contact	3	56.2	23.5																																				
Vulnerability to Attempted Acquisition of Technology via Foreign Visit	3	45.7	19.2																																				
Vulnerability to Exploitation of Commercial/Business Activities via Foreign Visit	3	45.8	19.2																																				
Vulnerability to Request for Information/Solicitation via Foreign Visit	1	7.5	7.5																																				
Vulnerability to Exploitation of Relationships via Foreign Visit	1	4.7	4.7																																				
Vulnerability to Request for Information/Solicitation via Conference, Conventions, or TradeShows	3	10.6	4.4																																				
Vulnerability to Exploitation of Cyber Operations via Personal Contact	3	10.4	4.4																																				
Vulnerability to Exploitation of																																							
Countermeasures	Creates aggregate list of all countermeasures, number of occurrences and their associated risk scores	Determining countermeasure status and the effect on risk	<p>Your Risk Overview [Show Legend]</p> <p>CURRENT Risk Level: 43% </p> <p>ORIGINAL Risk Level: 44.2% </p> <p>PLANNED Risk Level: 39.3% </p> <p>Risk Reduction by Countermeasure (3 assessments) - Double-click any row for breakout by assessment for that countermeasure</p> <table border="1"> <thead> <tr> <th>Category</th> <th>Mitigation</th> <th># Occurrences</th> <th>In Place</th> <th>Not In Place</th> <th>Max Risk Reduced</th> <th>Avg Risk Reduced</th> </tr> </thead> <tbody> <tr><td>CUI/CTI - Program Management (PM) - 01</td><td>The program shall develop and store in a secure facility all DoD technical data and computer software generated by the contract (e.g., source code, design drawings). All DoD technical data related to the contract and computer software generated by the contractor (e.g., source code, design drawings, etc.) for the program shall be developed and stored in a secure facility.</td><td>3</td><td>2</td><td>1</td><td>3.12%</td><td>2.06%</td></tr> <tr><td>CPI - Critical Program Information (CPI)/Anti-Tamper (AT) - 06</td><td>Personnel with access to classified design, manufacturing, or assembly information shall be trained on security classification markings, and dissemination controls.</td><td>3</td><td>2</td><td>1</td><td>3.12%</td><td>2.06%</td></tr> <tr><td>CLASSIFIED - Program Management (PM) - 02</td><td>The program shall employ Operations Security (OPSEC) safeguards, in</td><td>3</td><td>1</td><td>2</td><td>2.43%</td><td>2.20%</td></tr> </tbody> </table>	Category	Mitigation	# Occurrences	In Place	Not In Place	Max Risk Reduced	Avg Risk Reduced	CUI/CTI - Program Management (PM) - 01	The program shall develop and store in a secure facility all DoD technical data and computer software generated by the contract (e.g., source code, design drawings). All DoD technical data related to the contract and computer software generated by the contractor (e.g., source code, design drawings, etc.) for the program shall be developed and stored in a secure facility.	3	2	1	3.12%	2.06%	CPI - Critical Program Information (CPI)/Anti-Tamper (AT) - 06	Personnel with access to classified design, manufacturing, or assembly information shall be trained on security classification markings, and dissemination controls.	3	2	1	3.12%	2.06%	CLASSIFIED - Program Management (PM) - 02	The program shall employ Operations Security (OPSEC) safeguards, in	3	1	2	2.43%	2.20%								
Category	Mitigation	# Occurrences	In Place	Not In Place	Max Risk Reduced	Avg Risk Reduced																																	
CUI/CTI - Program Management (PM) - 01	The program shall develop and store in a secure facility all DoD technical data and computer software generated by the contract (e.g., source code, design drawings). All DoD technical data related to the contract and computer software generated by the contractor (e.g., source code, design drawings, etc.) for the program shall be developed and stored in a secure facility.	3	2	1	3.12%	2.06%																																	
CPI - Critical Program Information (CPI)/Anti-Tamper (AT) - 06	Personnel with access to classified design, manufacturing, or assembly information shall be trained on security classification markings, and dissemination controls.	3	2	1	3.12%	2.06%																																	
CLASSIFIED - Program Management (PM) - 02	The program shall employ Operations Security (OPSEC) safeguards, in	3	1	2	2.43%	2.20%																																	

Button	Description	Use For	Example																																																																																																																														
Risk Scenarios	Creates aggregate list of all asset to threat to vulnerability scenarios	Determining highest vulnerabilities and threats to assets.	<p>Aggregated Risk Scenarios</p> <p>Back</p> <p>Risk by Risk Scenario (3 assessments) - Double-click any row for breakout by assessment for that risk scenario</p> <table border="1"> <thead> <tr> <th>Threat Source</th> <th>Threat Method</th> <th>Vulnerability</th> <th>Asset Type</th> <th># Occurrences</th> <th>Max Risk Score</th> <th>Avg Risk Score</th> </tr> </thead> <tbody> <tr><td>Personal Contact</td><td>Exploitation of Relationship Vulnerability to Exploit Missiles</td><td></td><td></td><td>1</td><td>64.9</td><td>64.9</td></tr> <tr><td>Foreign Visit</td><td>Attempted Acquisition of Vulnerability to Attempted Missiles</td><td></td><td></td><td>1</td><td>52.7</td><td>52.7</td></tr> <tr><td>Foreign Visit</td><td>Exploitation of Commercial Vulnerability to Exploit Missiles</td><td></td><td></td><td>1</td><td>52.6</td><td>52.6</td></tr> <tr><td>Personal Contact</td><td>Exploitation of Relationship Vulnerability to Exploit Missiles</td><td></td><td>Programmable Memory</td><td>1</td><td>43.2</td><td>43.2</td></tr> <tr><td>Personal Contact</td><td>Exploitation of Relationship Vulnerability to Exploit Missiles</td><td></td><td>Field Programmable Gate J</td><td>1</td><td>43.2</td><td>43.2</td></tr> <tr><td>Personal Contact</td><td>Exploitation of Relationship Vulnerability to Exploit Missiles</td><td></td><td>Aircraft &amp; Design</td><td>2</td><td>64.9</td><td>38.3</td></tr> <tr><td>Personal Contact</td><td>Exploitation of Relationship Vulnerability to Exploit Missiles</td><td></td><td>Unmanned Aerial Vehicles</td><td>2</td><td>64.9</td><td>36.7</td></tr> <tr><td>Foreign Visit</td><td>Attempted Acquisition of Vulnerability to Attempted Field Programmable Gate J</td><td></td><td></td><td>1</td><td>35.1</td><td>35.1</td></tr> <tr><td>Foreign Visit</td><td>Exploitation of Commercial Vulnerability to Exploit Missiles</td><td></td><td>Programmable Memory</td><td>1</td><td>35.1</td><td>35.1</td></tr> <tr><td>Foreign Visit</td><td>Exploitation of Commercial Vulnerability to Exploit Missiles</td><td></td><td>Field Programmable Gate J</td><td>1</td><td>35.1</td><td>35.1</td></tr> <tr><td>Foreign Visit</td><td>Attempted Acquisition of Vulnerability to Attempted Programmable Memory</td><td></td><td></td><td>1</td><td>35.1</td><td>35.1</td></tr> <tr><td>Foreign Visit</td><td>Exploitation of Commercial Vulnerability to Exploit Missiles</td><td></td><td>Aircraft &amp; Design</td><td>2</td><td>52.6</td><td>31.3</td></tr> <tr><td>Foreign Visit</td><td>Attempted Acquisition of Vulnerability to Attempted Aircraft &amp; Design</td><td></td><td></td><td>2</td><td>52.7</td><td>31.3</td></tr> <tr><td>Foreign Visit</td><td>Attempted Acquisition of Vulnerability to Attempted Unmanned Aerial Vehicles</td><td></td><td></td><td>2</td><td>52.7</td><td>29.9</td></tr> <tr><td>Foreign Visit</td><td>Exploitation of Commercial Vulnerability to Exploit Missiles</td><td></td><td>Unmanned Aerial Vehicles</td><td>2</td><td>52.6</td><td>29.8</td></tr> <tr><td>Conference, Conventions, Request for Information/Si</td><td>Request for Information/Si Vulnerability to Request for Missiles</td><td></td><td></td><td>1</td><td>12.2</td><td>12.2</td></tr> <tr><td>Personal Contact</td><td>Exploitation of Cyber Oper Vulnerability to Exploit Missiles</td><td></td><td></td><td>1</td><td>11.9</td><td>11.9</td></tr> </tbody> </table> <p>Rows 1 - 50 of 352</p>	Threat Source	Threat Method	Vulnerability	Asset Type	# Occurrences	Max Risk Score	Avg Risk Score	Personal Contact	Exploitation of Relationship Vulnerability to Exploit Missiles			1	64.9	64.9	Foreign Visit	Attempted Acquisition of Vulnerability to Attempted Missiles			1	52.7	52.7	Foreign Visit	Exploitation of Commercial Vulnerability to Exploit Missiles			1	52.6	52.6	Personal Contact	Exploitation of Relationship Vulnerability to Exploit Missiles		Programmable Memory	1	43.2	43.2	Personal Contact	Exploitation of Relationship Vulnerability to Exploit Missiles		Field Programmable Gate J	1	43.2	43.2	Personal Contact	Exploitation of Relationship Vulnerability to Exploit Missiles		Aircraft & Design	2	64.9	38.3	Personal Contact	Exploitation of Relationship Vulnerability to Exploit Missiles		Unmanned Aerial Vehicles	2	64.9	36.7	Foreign Visit	Attempted Acquisition of Vulnerability to Attempted Field Programmable Gate J			1	35.1	35.1	Foreign Visit	Exploitation of Commercial Vulnerability to Exploit Missiles		Programmable Memory	1	35.1	35.1	Foreign Visit	Exploitation of Commercial Vulnerability to Exploit Missiles		Field Programmable Gate J	1	35.1	35.1	Foreign Visit	Attempted Acquisition of Vulnerability to Attempted Programmable Memory			1	35.1	35.1	Foreign Visit	Exploitation of Commercial Vulnerability to Exploit Missiles		Aircraft & Design	2	52.6	31.3	Foreign Visit	Attempted Acquisition of Vulnerability to Attempted Aircraft & Design			2	52.7	31.3	Foreign Visit	Attempted Acquisition of Vulnerability to Attempted Unmanned Aerial Vehicles			2	52.7	29.9	Foreign Visit	Exploitation of Commercial Vulnerability to Exploit Missiles		Unmanned Aerial Vehicles	2	52.6	29.8	Conference, Conventions, Request for Information/Si	Request for Information/Si Vulnerability to Request for Missiles			1	12.2	12.2	Personal Contact	Exploitation of Cyber Oper Vulnerability to Exploit Missiles			1	11.9	11.9
Threat Source	Threat Method	Vulnerability	Asset Type	# Occurrences	Max Risk Score	Avg Risk Score																																																																																																																											
Personal Contact	Exploitation of Relationship Vulnerability to Exploit Missiles			1	64.9	64.9																																																																																																																											
Foreign Visit	Attempted Acquisition of Vulnerability to Attempted Missiles			1	52.7	52.7																																																																																																																											
Foreign Visit	Exploitation of Commercial Vulnerability to Exploit Missiles			1	52.6	52.6																																																																																																																											
Personal Contact	Exploitation of Relationship Vulnerability to Exploit Missiles		Programmable Memory	1	43.2	43.2																																																																																																																											
Personal Contact	Exploitation of Relationship Vulnerability to Exploit Missiles		Field Programmable Gate J	1	43.2	43.2																																																																																																																											
Personal Contact	Exploitation of Relationship Vulnerability to Exploit Missiles		Aircraft & Design	2	64.9	38.3																																																																																																																											
Personal Contact	Exploitation of Relationship Vulnerability to Exploit Missiles		Unmanned Aerial Vehicles	2	64.9	36.7																																																																																																																											
Foreign Visit	Attempted Acquisition of Vulnerability to Attempted Field Programmable Gate J			1	35.1	35.1																																																																																																																											
Foreign Visit	Exploitation of Commercial Vulnerability to Exploit Missiles		Programmable Memory	1	35.1	35.1																																																																																																																											
Foreign Visit	Exploitation of Commercial Vulnerability to Exploit Missiles		Field Programmable Gate J	1	35.1	35.1																																																																																																																											
Foreign Visit	Attempted Acquisition of Vulnerability to Attempted Programmable Memory			1	35.1	35.1																																																																																																																											
Foreign Visit	Exploitation of Commercial Vulnerability to Exploit Missiles		Aircraft & Design	2	52.6	31.3																																																																																																																											
Foreign Visit	Attempted Acquisition of Vulnerability to Attempted Aircraft & Design			2	52.7	31.3																																																																																																																											
Foreign Visit	Attempted Acquisition of Vulnerability to Attempted Unmanned Aerial Vehicles			2	52.7	29.9																																																																																																																											
Foreign Visit	Exploitation of Commercial Vulnerability to Exploit Missiles		Unmanned Aerial Vehicles	2	52.6	29.8																																																																																																																											
Conference, Conventions, Request for Information/Si	Request for Information/Si Vulnerability to Request for Missiles			1	12.2	12.2																																																																																																																											
Personal Contact	Exploitation of Cyber Oper Vulnerability to Exploit Missiles			1	11.9	11.9																																																																																																																											
Reports	Takes user to reports page where further reports are listed	Further detail on countermeasure status, graphs and images for presentations.	<p>Home &gt; Advanced Analysis &gt; Reports</p> <p><b>EPRM will prepare reporting data for you.</b></p> <p>Reporting data, in various formats and configurations, can be generated to include in your reports. This allows users to select the appropriate type and format of data for different reports and presentations.</p> <p><a href="#">Multi-Assessment Analysis (XLSX)</a> Creates a multi-tab spreadsheet-based report that provides a comprehensive view of asset, threat and countermeasure status and presents data and charts to measure risk by asset, threat or location for a collection of assessments.</p> <p><a href="#">Countermeasure Compliance Implementation and Analysis (XLSX)</a> Creates an Excel analysis datasheet detailing the status of countermeasures implementation across the selected assessments.</p> <p><a href="#">Risk Scenarios (XLSX)</a> Generates a table of all risk scenarios.</p> <p>Back</p>																																																																																																																														

Button	Description	Use For	Example
Dashboard	Generates Excel file showing aggregate risk, and the status of the Program Protection Plan	At a glance reporting of Risk and Program Protection. This is one of the key reports of ASM.	<p>The dashboard displays three main sections:</p> <ul style="list-style-type: none"> <li><b>Program Security Risk Reduction:</b> A gauge chart showing risk levels from 0% to 100%. The needle is positioned at approximately 75%.</li> <li><b>Program Protection Plan Compliance:</b> A bar chart showing compliance status for various categories. Categories include Critical Program Information (CPI) &amp; Anti-Sampler (AS), Criticality Analysis (CA), Correct Language, Intelligence Support, Software Analysis (SA), and Signed FPP. Most categories show green bars (Yes), except for CPI &amp; AS which shows a red bar (No).</li> <li><b>Program Security Risk and Remediation:</b> A table titled 'TEST EXEC SUMMARY' showing Current and Planned counts for various risk levels (Low, Medium, High, Very High). All counts are 15.</li> </ul>

Figure 86: Advanced Analysis: Table of Example Reports

## 8 View References and Materials

The Reference and Materials section has documents relative to all EPRM modules. This includes DOD references, job aids, frequently asked questions and other information.

The screenshot shows a software interface with a top navigation bar and a main content area. The top bar has a 'Main Menu' button and four icons: 'Manage Assessments' (blue), 'Advanced Analysis' (red), 'Manage Survey Responses' (green), and 'View References and Materials' (yellow). The 'View References and Materials' icon is highlighted with a red box. Below the bar, the main content area has a header 'Home > References and Materials'. It features a welcome message: 'Welcome to your Reference and Materials Library! Here you will find many useful reference documents to help you support and develop your own Risk Assessment plan, or improve an existing Risk Assessment plan. Each picture below contains documents, policies, templates, or other references to help you in the Risk Assessment Process.' It also includes a note: 'Click on any of the links to access references in that group.' A 'Help' icon (question mark) is shown next to a link: 'Having some trouble? Take a look at the EPRM [frequently asked questions](#)'. Below this, it says 'Listed below are some reference documents to help build your Risk Analysis program.' There are two 'Back' buttons at the bottom right of the content area.

Figure 87: References and Materials

## 9 ASM Dedicated Help Page

The ASM portal has all user guides, job aids, questions lists and other material to assist users in the ASM process. Use this link to access: <http://eprmhelp.countermeasures.com/ASM>



Figure 88: ASM Dedicated Help Page

Section	Description/Content
<b>Get Started</b>	Login request form Steps to get started
<b>Training Resources</b>	User Guide Job Aids Computer Based Training (CBT)
<b>Marketing, Communications and Policy</b>	ASM Overview Senior Level video End User Informational Video ASM Business Rules
<b>FAQs</b>	Hyperlink format; Answers to Frequently asked questions
<b>Quick Links to Communications</b>	Current news and links

Figure 89: ASM Dedicated Help Page Contents

## 10 ASM Demo Account

### Purpose

The ASM demo account is a mirror of the functionality on SIPRNet but with a different hierarchy set up and notional data. The SIPR and NIPR databases are separate and different. This unclassified site facilitates user familiarization and training. **Users shall not use the demo site to create any real assessments.**

Assessments created in the demo site will not show in the SIPRNet site. In addition:

- The Alion Help desk will set up hierarchy/assessment/user administrators at the PEO level.
- Node and System Administrators may further delegate within their branch of the hierarchy.
- This site CANNOT be used for unclassified assessment question exports for SIPRNet.
- The headers of the training site will clearly state “Training Data”.
- The demo site may be periodically purged of data when system upgrades or space limitations dictate. ASM leads will be notified well in advance of any changes/removal of training assessment data.

### Access

The site is at <http://demo.countermeasures.com>. Users can access the training site by clicking on the EPRM button labeled with the current EPRM version, (e.g., EPRM 3.30). ASM will automatically direct users to the ASM module.

## Getting a login for the demo account

Provide the following information to the EPRM Help Desk via email at [eprmhelpdesk@alionscience.com](mailto:eprmhelpdesk@alionscience.com)

Note: If you have requested a SIPRNet ASM account, the Helpdesk will also add you to the Demo account.

Name:				
Title/ Rank:				
Phone number:				
Service or Component:	<b>Air Force</b>			
Center (i.e., AFLNWC)				
Two letter Directorate (i.e., ND)				
Three letter Program (i.e., ND1)				
Program Executive Officer (PEO)				
Alion Contract Name:	<b>Acquisition Security</b>			
NIPR E-Mail:				
SIPR E-Mail:				
<b><i>ALL Users will be put in Demo and SIPR ASM and assigned the role of Assessor and Assessment Manager at their three-digit level unless otherwise noted by Approving Official</i></b>				
<b><i>THE FOLLOWING INFORMATION WILL BE COMPLETED BY APPROVING OFFICIAL AND THE EPRM HELP DESK</i></b>				
(Add "X" next to applicable level)				
<b>Role(s)</b>	X Assessor	Assessment Mgr.		
(Add "X" next to applicable level)				
<b><i>The following roles require additional approval</i></b>				
Templator	Template Mgr	Node Admin	User Admin	Observer