**Scan Results Processor (SRP)**

**USER’S MANUAL**

*Robert Sakey*

RMF Version 1.2.2: April 18, 2017

**Revision Sheet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Release No.** | **Date** | **Revision Description** | **Author** |
| 1.0.0 | 3/5/2017 | Initial Release | Robert Sakey |
| 1.0.1 | 3/14/2017 | Changes to Security Controls and Assessment Procedures | Robert Sakey |
| 1.1.0 | 3/24/2017 | First major production version | Robert Sakey |
| 1.2.0 | 4/04/2017 | Added export buttons for SC and AP forms, added Tier 3 Inheritance, changed Overlay buttons | Robert Sakey |
| 1.2.1 | 4/7/2017 | Changed STIG Viewer Import to automatically test for version | Robert Sakey |
| 1.2.2 | 4/18/2017 | Minor fixes. First use of Back End Updater | Robert Sakey |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**TABLE OF CONTENTS**

[1 Introduction 5](#_Toc480277575)

[1.1 Purpose 5](#_Toc480277576)

[1.2 Scope 5](#_Toc480277577)

[2 Getting Started 5](#_Toc480277578)

[2.1 System Requirements 5](#_Toc480277579)

[2.2 Scan Results Processor Contents and Description 5](#_Toc480277580)

[2.3 Installation 6](#_Toc480277581)

[2.3.1 Install Scan Results Processor 6](#_Toc480277582)

[2.3.2 Copy SRP to Working Directory 6](#_Toc480277583)

[2.4 Starting the Scan Results Processor 6](#_Toc480277584)

[3 MainGui 7](#_Toc480277585)

[3.1 Back End Databases 8](#_Toc480277586)

[3.2 Setup Form 9](#_Toc480277587)

[3.2.1 Setup data 9](#_Toc480277588)

[3.2.2 Security Controls 9](#_Toc480277589)

[3.2.3 Assessment Procedures 9](#_Toc480277590)

[3.2.4 POA&M 9](#_Toc480277591)

[3.2.5 Form Color 10](#_Toc480277592)

[3.2.6 Procedure Paint On/Off 10](#_Toc480277593)

[3.2.7 AutoBackup 10](#_Toc480277594)

[3.2.8 Control Selection 10](#_Toc480277595)

[3.2.8.1 800-53 Control Selection 10](#_Toc480277596)

[3.2.8.2 Setup Overlays 10](#_Toc480277597)

[3.2.8.3 Open Controls Report 12](#_Toc480277598)

[3.2.8.4 Open Controls Report - Details 12](#_Toc480277599)

[3.2.8.5 Open Controls Report - Procedures 12](#_Toc480277600)

[3.2.8.6 Open IA Controls Report 12](#_Toc480277601)

[3.2.8.7 Open Form 12](#_Toc480277602)

[3.2.8.8 Open Common Controls Report 12](#_Toc480277603)

[3.2.8.9 Remove Additional Controls 12](#_Toc480277604)

[3.2.9 Update CCIs 12](#_Toc480277605)

[3.2.10 Clear Database 12](#_Toc480277606)

[3.2.11 Baseline 12](#_Toc480277607)

[3.2.12 Relink Database 13](#_Toc480277608)

[3.3 Backend Backup 13](#_Toc480277609)

[3.4 Exit 14](#_Toc480277610)

[3.5 Compact Off/On 14](#_Toc480277611)

[3.6 IAVM 14](#_Toc480277612)

[3.6.1 Project Form 14](#_Toc480277613)

[3.6.2 IAVM Forms 15](#_Toc480277614)

[3.6.3 IAVM Reports 16](#_Toc480277615)

[3.6.4 Import IAVMs 17](#_Toc480277616)

[3.7 Security Plan 17](#_Toc480277617)

[3.8 Security Controls 17](#_Toc480277618)

[3.9 Assessment Procedures 18](#_Toc480277619)

[3.10 Plan of Action & Milestones 19](#_Toc480277620)

[3.11 Update POA&M 20](#_Toc480277621)

[3.12 Scan Summary 20](#_Toc480277622)

[3.13 Scan Results 22](#_Toc480277623)

[3.13.1 Viewing Vulnerabilities 23](#_Toc480277624)

[3.13.2 Updating Vulnerabilities 23](#_Toc480277625)

[3.13.3 Dealing with Vulnerabilities that are Open on one Host and Closed on Another 25](#_Toc480277626)

[3.13.4 Scan Results Report 25](#_Toc480277627)

[3.13.5 Missing Controls 26](#_Toc480277628)

[3.13.6 Procedure Paint On/Off 27](#_Toc480277629)

[3.13.7 Closing the Scan Results Form 27](#_Toc480277630)

[3.14 All Scan Results 27](#_Toc480277631)

[3.14.1 All Scan Results Report 27](#_Toc480277632)

[3.14.2 Click to Show Only Latest Scans 27](#_Toc480277633)

[3.14.3 Missing Controls 27](#_Toc480277634)

[3.15 Import Data 27](#_Toc480277635)

[3.16 Forms & Reports 30](#_Toc480277636)

[3.16.1 Scans Form 30](#_Toc480277637)

[3.16.2 Software List 30](#_Toc480277638)

[3.16.3 Hardware List 31](#_Toc480277639)

[3.16.4 PPS List 31](#_Toc480277640)

[3.16.5 Test Plan 31](#_Toc480277641)

[3.16.6 Inheritance List 31](#_Toc480277642)

[3.16.7 Mitigated Vulnerabilities List 32](#_Toc480277643)

[3.16.8 N/A Security Controls List 32](#_Toc480277644)

[3.16.9 FISMA Report 32](#_Toc480277645)

[3.16.10 All Open Scans Results Report 33](#_Toc480277646)

[3.16.11 Multiple Hosts Findings Report 34](#_Toc480277647)

[3.16.12 Vulnerabilities by Security Controls Report 35](#_Toc480277648)

[3.16.13 Vulnerability Count Report 36](#_Toc480277649)

[3.16.14 Vulnerability Count Report per Checklist 37](#_Toc480277650)

[3.16.15 Vulnerability Count Report per Checklist – No Severity 37](#_Toc480277651)

[3.16.16 eMASS Risk Assessment Report (RAR) 38](#_Toc480277652)

[3.16.17 eMASS POA&M Import (All Ongoing Findings) 38](#_Toc480277653)

[3.16.18 eMASS POA&M Import (Baselined Ongoing Findings) 38](#_Toc480277654)

[3.16.19 eMASS POA&M Import (New Findings Since Baseline) 38](#_Toc480277655)

[3.16.20 eMASS POA&M Import (Closed Findings Since Baseline) 38](#_Toc480277656)

[3.16.21 eMASS Test Result Import 38](#_Toc480277657)

[3.16.22 eMASS Implementation Plan (Assigned Security Controls) 38](#_Toc480277658)

[3.16.23 eMASS Risk Assessment Summary 38](#_Toc480277659)

[3.16.24 eMASS Security Assessment Report (SAR) Sheet 1 39](#_Toc480277660)

[3.16.25 eMASS Security Assessment Report (SAR) Sheet 2 39](#_Toc480277661)

[3.16.26 CD Totals 39](#_Toc480277662)

[4 Troubleshooting 40](#_Toc480277663)

[4.1 Windows 7 40](#_Toc480277664)

[4.2 Microsoft Office 2007 40](#_Toc480277665)

[4.3 Verify data is correct 41](#_Toc480277666)

[4.4 Compact and Repair 41](#_Toc480277667)

[4.5 Changing Data Issues 41](#_Toc480277668)

[4.1 Database goes to code window when opening for the first time. 41](#_Toc480277669)

[5 Point of Contact 41](#_Toc480277670)

[6 Revision History 41](#_Toc480277671)

[6.1 1.0.0 41](#_Toc480277672)

[6.2 1.0.1 41](#_Toc480277673)

[6.3 1.1.0 41](#_Toc480277674)

[6.4 1.2.0 42](#_Toc480277675)

[6.5 1.2.1 42](#_Toc480277676)

[6.6 1.2.2 42](#_Toc480277677)

# Introduction

The Cybersecurity (CS) community uses numerous tools to test, scan, document, and present an information system’s security posture under the Risk Management Framework (RMF). The Scan Results Processor (SRP) provides an automated means to process, document, and present the raw data captured in the various CS testing, scans, and checklists. SRP provides the processed data in the format and on the forms required in RMF.

## Purpose

This user’s manual details the procedures necessary for the use and operation of the SRP tool.

## Scope

The original SRP was a government owned tool that may be used by any DoD government entity at no charge. Following in that tradition, this modification to the SRP is available free of charge. No license is required. The tool is designed around the Navy RMF process and provides data in established forms and formats.

# Getting Started

## System Requirements

* Microsoft Office 2010 or newer
  + Scan Results Processor database built with Access 2013 and may require work-arounds to work in older versions of Access (see troubleshooting section)
* STIG Viewer (optional)
  + Tool for aggregation of security findings for systems
  + Located on the iase.disa.mil website
  + Currently supports versions 1.2, 2.3.x and 2.4.1
* ACAS (optional)
  + Tool for scanning Windows, Linux and UNIX computers
  + Located on the iase.disa.mil website
* 200 MB of free hard drive space
  + Capacity to host SRP files as well as scan data
  + Installation requires 25 MB of free hard drive space
  + The back end database starts at 14 MB and can grow considerably after importing scans

## Scan Results Processor Contents and Description

* Scan Results Processor – RMF x.x.x.accdb
  + Front end database file used for importing, processing, and display of scan data.
  + Can be overwritten with new versions
* Scan Results Processor – RMF x.x.x be.accdb
  + Back end database file used for storing scan data.
  + Should not be overwritten with new versions
* POAM.xlsx.
  + Template spreadsheet to export Plan of Actions and Milestones data from SRP.
* ManualScansTemplate.xlsx
  + Template spreadsheet for inputting Manual Scan data, when no xml STIG is available (e.g. Dot Net Framework 1 to 3.5).

## Installation

### Install Scan Results Processor

Run the executable file called Scan Results Processor.exe. Two separate databases with different file names will be created, a front end and a back end database. The front end database is called Scan Results Processor – RMF x.x.x.accdb and the back end database is called Scan Results Processor – RMF x.x.x be.accdb. These two database files will be placed in the folder named C:\Scan Results Processor. The databases can be renamed later for convenience. It is suggested that the following convention be used for naming the front and back end databases. Front End = “Name.accdb”. Back End = “Name be.accdb”. You must put a space between the “name” and the “be” parts.

### Copy SRP to Working Directory

The Scan Results Processor can be run from the installation folder or a different folder. For configuration management reasons an instance of the SRP should be copied to a different working directory. It is recommended that the SRP folder be set as a Microsoft Trusted Location (not available on NMCI). Separate versions of the SRP can be installed for each project in separate directories. For example, if you have two versions of a system that would produce two separate POA&Ms, etc. The POAM template should be copied to each working directory. When upgrading to a newer version of SRP, make sure to only copy over the front end. The front end database is designed to make changes to the back end database without affecting the already existing data.

\*Note: Do not “move” the database, “Copy” it. This will make it easier to relink the front end and back end databases. If the linked back end database is not found, the front end will attempt to link to a database with the same name plus “ be”. With the use of the Select BackEnd functionality, it is easy to use one front end that can easily connect to multiple back end databases. The POAM template should be in the same folder as the front end database.

## Starting the Scan Results Processor

* Navigate to the location of the SRP in the working directory.
* Double-click the “Scan Results Processor.accdb” icon.

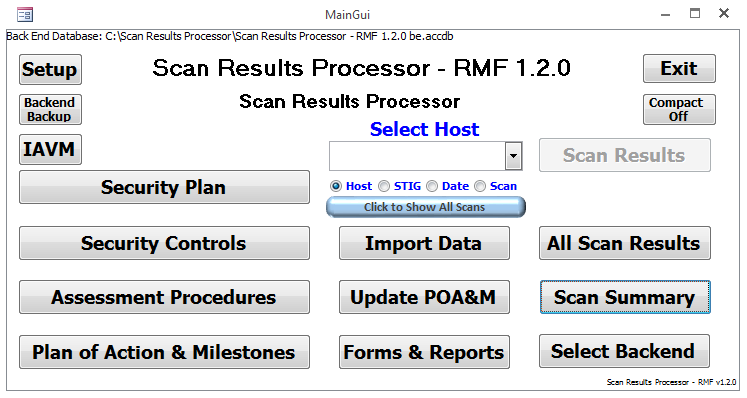


When first opened, the database will execute an update of the back end database if any changes have been made. This would only occur when using a newer version of the front end. Click the Yes button and the back end database will update. If there are a lot of updates, you may see the following screen. 

Then Microsoft (MS) Access will execute and open up the database file to the Main graphical user interface (GUI) form.

# MainGui

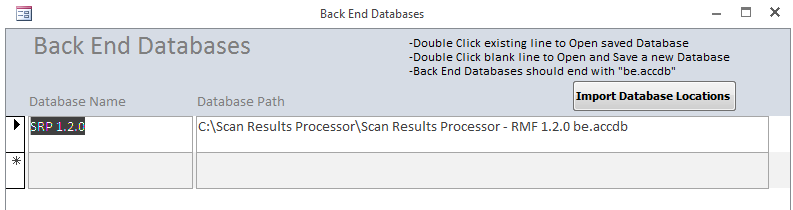
The MainGui will be the base of operations for the SRP.



**Example of the Scan Results Processor MainGui Page**

## Back End Databases

Take note of the location of the back end database, which is shown at the top of the window. If you want to connect to a different back end database, click the Select Backend button.



The Back End Databases form allow the user to select or add back end databases. Double clicking in either the Database Name or Database Path field for an existing record will load the back end database chosen. Double clicking in either the Database Name or Database Path field for a new record will bring up the Windows File Open dialog box allowing the user to choose the location of the back end database. If new tables have been created in newer versions of the database, then it is possible to get an expected error similar to the following:



Enter a name for the back end database selected in the Back End Database Nickname form.



Successful links will generate the following message:

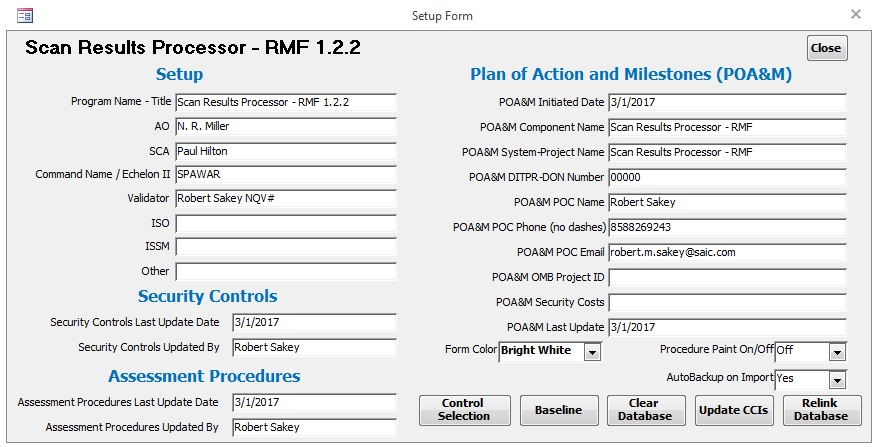


New versions of the front end database do not have the Back End Database records found in the Back End Databases form. To import the back end databases, click on the Import Database Locations button (twice). Select the location of a front end database from the Microsoft File Open dialog. After import, this message will display:



## Setup Form

From the MainGui form, click the **Setup** button to open the Defaults Form.



**Example of the Defaults Form**

### Setup data

Enter Setup information. The Program Name – Title will appear on the MainGui and many reports and windows within the SRP.

### Security Controls

Enter Last Update Date and Updated By information for the Security Controls.

### Assessment Procedures

Enter Last Update Date and Updated By information for the Assessment Procedures.

### POA&M

Enter POA&M information. This information is typically found in the header of the POA&M.

### Form Color

This drop down box allows the user to select the color of the MainGui.

### Procedure Paint On/Off

This drop down box turns the color on or off for the Assessment Procedures button on the Scan Results Form. This drop down box also exists on the Scan Results Form. It is recommended that this be kept at “Off” or “0” for normal operations.

### AutoBackup

This drop down box sets the status for Auto Backup when importing scans. When set to “Yes”, an automatic backup of the backend database will be created. When set to “No” an automatic backup of the backend database will not be created. The default value is “Yes”.

### Control Selection

This allows the selection of Controls, Assessment Procedures and Overlays.

#### 800-53 Control Selection

Select Confidentiality, Integrity and Availability levels. Closing the selection window will reset the applicable Security Controls after clicking Yes on the following message:



**Note: This will remove any applied Overlays.**

#### Setup Overlays

If you need to apply overlays, first make changes to the Security Controls, exit the Selection window, then return to the Control Selection and click on Setup Overlays.



Green highlight shows the applicability of the specific overlay. For example, the applicability of the Classified and Privacy Overlays above shows for AC-11 and AC-20(3). The Yes field for each control is highlighted along with the Classified row of data (top row) and the Privacy row of data (second row). Not all Overlays have Control Text, Supplemental Guidance or Parameter Values, which is why there are highlighted blank fields. Select an Overlay by clicking the specific Apply Overlay button. The text and color of the button changes depending on whether an overlay has been applied or not. You can click more than one. A message will pop up every time an Overlay is applied. Do not apply both Cybersafe A and Cybersafe B.



#### Open Controls Report

The Open Controls Report shows a list of Security Controls associated with the selected Confidentiality, Integrity and Availability

#### Open Controls Report - Details

The Open Controls Report – Details shows a list of Security Controls associated with the selected Confidentiality, Integrity and Availability along with Control Text and Supplemental Guidance.

#### Open Controls Report - Procedures

The Open Controls Report - Procedures shows a list of Assessment Procedures associated with the selected Confidentiality, Integrity and Availability along with CCIs, CCI Definitions, Implementation Guidance and Assessment Procedures.

#### Open IA Controls Report

The Open IA Controls Report shows a list of Security Controls associated with the selected Confidentiality, Integrity and Availability mapped to associated IA Controls.

#### Open Form

The 800-53 Controls Form shows the data associated with the Security Controls. It also allows the user to add additional controls by putting the letter “A” into any blank CIA field. Make sure to also put a “Y” into the Selected Control field.

#### Open Common Controls Report

The Open Common Controls Report shows a list of Security Controls associated with the selected Confidentiality, Integrity and Availability and which ones are Common Controls.

#### Remove Additional Controls

The Remove Additional Controls will remove the letter “A” from the 800-53 Controls Form. Removing the “Y” from the Selected Control field will require the user to close out and select the “Yes” from the Seet Security Controls dialog box.

### Update CCIs

This updates the relationship between vulnerabilities found in STIGs and CCIs. This is updated every quarter with the release of a new STIG zip compilation file. This requires the existence of a specially compiled csv file named “SRPCCIUpdate.csv”. More information to follow.

### Clear Database

This clears all data from the backend database. Be judicial about doing this.

### Baseline

This marks findings as baselined. Differences between baselined and non-baselined findings can be found in a report. This will allow the user to create a POAM import file that only has new findings in it from the last time a baseline was created in eMASS.

### Relink Database

If the Scan Results Processor was moved or renamed, then the first thing that should be done is to relink the database. This is rarely needed as the Select Backend functionality from the MainGuid should take care of all issues. The Relink Database button allows the user to link the front end database to the back end database in case the back end database is moved or its name is changed. It is suggested that the user make a copy of the back end database first then either move or rename the copy. Then while the front end database is pointing to the old back end database, the user can change the links.



**Example of the Linked Table Manager Form**

In the Linked Table Manager, select the Always prompt for new location check box. Click the Select All button. Click the OK button. Select the location of the back end database.



After all linked table are successfully refreshed, click the close button.

Click the **Close** button in the upper right to exit and return to the MainGui Form.

\*\*Note: After relinking a database, the user should restart the database before adding any data to the Defaults form.

## Backend Backup

The Backend Backup button allows a quick way of making a copy of the backend database.



## Exit

It is preferable to use the Exit button to exit the database.

## Compact Off/On

The Compact Off/On button allows the user to select whether the database will be compacted after clicking the Exit button. It is recommended that the database be compacted at least weekly. This does not compact the back end database. To compact the back end database. Close the front end database. Open the back end database to be compacted. Select Database Tools from the menu then select Compact and Repair Database from the Microsoft Office ribbon. Then click the Exit Database button to exit. The back end database will grow considerably with each import. A compact will reduce the size of the database.

## IAVM

The IAVM button allows the user to access optional Information Assurance Vulnerability Management functionality.



The IAVM Main form allows the user to access IAVM Forms, IAVM Reports, the Project Form, and the ability to import IAVAs and IAVBs.

### Project Form

The Project Form is a list of Projects or Components of the system.



### IAVM Forms

Clicking on the IAVM Forms button opens the IAVM Form Selection Form.



Select an IAVM Status of either Active or All. All is the default value if nothing is selected. Then select either the Open IAVM Form button or the Open IAVM Project Form.





The IAVM Project Form shows all IAVs associated with Projects/Components. One row for each IAV/Project/Component. Entering check marks in the Applicable, Lab Applied, and Deployed check boxes will mark the IAVs different colors: Gray for Not Applicable (default), Red for Applicable but not Applied, Yellow for Applicable and Applied in the Lab, but not Deployed, and Green for Deployed.

### IAVM Reports

Clicking on the IAVM Reports button opens the IAVM Report Selection Form.



Select an IAVM Status of either Active or All. Select an Applicable of Applicable or All. All is the default value if nothing is selected. Then select either the Open IAVM Report button or the Open IAVM Project Report. When selecting Applicable in the Applicable drop down box, the IAVM Project Report will filter for only those IAVMs that are checked as Applicable.





The IAVM Project Report shows all IAVs associated with Projects/Components. One row for each IAV/Project/Component. Entering check marks in the Applicable, Lab Applied, and Deployed check boxes on the IAVM Project Form will mark the IAVs different colors on this report: Gray for Not Applicable, Red for Applicable but not Applied, Yellow for Applicable and Applied in the Lab, but not Deployed, and Green for Deployed.

### Import IAVMs

The Import IAVMs button will run code that will import the latest iavms.xls from the IAVM web site. Make sure that the iavm.xls file is located in the same directory of the front end database. The file can be downloaded from <https://iavm.csd.disa.mil/>. Click the Notices button, then click Search Notices. From the Search IAVM Notices screen, check the Include non-active notices check box, then click the Download Excel Summary button. This will download a full list of all IAVs as iavm.xls.

Also, click this button if any changes are made to the Project/Component form.

## Security Plan

The Security Plan matches the fields for the Security Plan in eMASS. You should only create one record for this form.

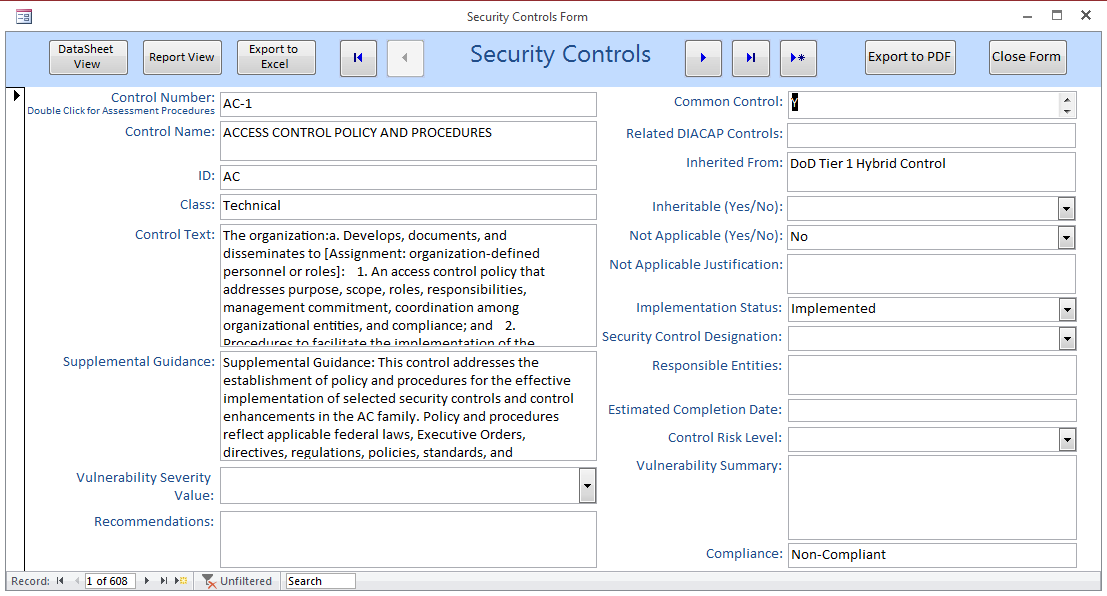
The DataSheet View button allows the user to enter and review data in a spreadsheet format. The Report View allows the user to create a report of the Security Plan.

## Security Controls

The Security Controls Form allows the user to provide status for selected security controls. Many of the fields on this form are required for other reports. Entering any data in the Inherited From field automatically marks that Security Control and its associated Assessment Procedures as Inherited. Deleting any value in the Inherited From field automatically removes the inheritance from that Security Control and its associated Assessment Procedures. Selecting “Yes” in the Not Applicable field will also mark all associated Assessment Procedures as Not Applicable. Selecting “No” in the Not Applicable field will mark all associated Assessment Procedures as not Not Applicable.

Changes to the Inherited From, Inheritable, Not Applicable and Not Applicable Justification fields overwrite the same fields on the Assessment Procedures Form. If the Inherited From field on the Assessment Procedures Form has “Tier 1” or “Tier 2” in it, it will not be updated, as these need to be updated manually.

The DataSheet View button allows the user to enter and review data in a spreadsheet format. The Report View allows the user to create a report of the Security Controls. The Export to Excel button will export the Security Controls query to Excel. To change the format of the export for the future, edit the Security Controls.xlsx file in the same folder as the front end database. The Export to PDF button will create a pdf of the Report presented in the Report View.



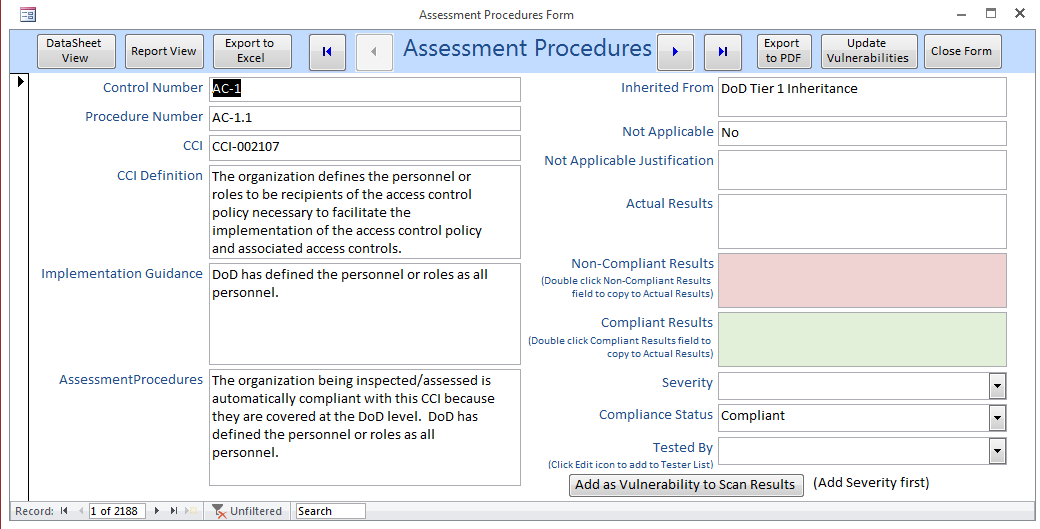
## Assessment Procedures

The Assessment Procedures Form allows the user to provide status for assessment procedures associated with selected security controls. Many of the fields on this form are required for other reports. Entering any data in the Inherited From field does not automatically mark that Security Control as Inherited. Deleting any value in the Inherited From field does not automatically remove the inheritance from that Security Control. Selecting “Yes” in the Not Applicable field will not mark the associated Security Control as Not Applicable. Selecting “No” in the Not Applicable field will not mark the associated Security Control as not Not Applicable.

After scans are imported, a concatenation of all the open findings associated with a particular Assessment Procedure can be created in the Vulnerability field by clicking the Update Vulnerabilities button. The same will be done for closed findings in the Non-Vulnerability field.

Clicking the **Add as Vulnerability to Scan Results** button will add the procedure as a vulnerability to the scan results with a ScanID of 1 and Host name of 800-53 Rev4. The Severity needs to be added first. This allows any of the Assessment Procedures to be added as a Vulnerability and treated like any other vulnerability on a STIG.

The DataSheet View button allows the user to enter and review data in a spreadsheet format. The Report View allows the user to create a report of the Assessment Procedures. The Export to Excel button will export the Assessment Procedures query to Excel. To change the format of the export for the future, edit the Assessment Procedures.xlsx file in the same folder as the front end database. The Export to PDF button will create a pdf of the Report presented in the Report View.



## Plan of Action & Milestones

The POA&M can be opened by clicking the **Plan of Action & Milestones** button on the MainGui. This report is comparable to the old System POA&M. The POA&M is opened in Report View in MS Access rather than the normal Print Preview. This allows the user to scroll through findings and export the results to an Excel Spreadsheet. The user can, of course, print this report by clicking **Print**. Understand that this is the full list of all vulnerabilities in the system, Open, Closed and N/A.

Because MS Access tends to truncate data to 255 characters per field, an export to Excel capability has been added to the SRP. A POAM.xlsx file has been included with the SRP. It is pre-formatted and must exist in the same folder as the front end database. Click **Export POA&M to Excel** and the POA&M will be exported. The POA&M.xlsx file is then opened to a tab labeled “qry\_POAM\_Export”. Changes can be made to the format of this document and it will stay formatted for the next export. Just make sure not to rename the tab or to delete the POAM Range. It is always a good idea to copy exports to a different folder. It is recommended to delete all the data on the form before each export as data will overwrite cells, not delete and then write. If you had 1000 lines of data saved in the POAM.xlsx file and then exported again with 500 items, there will still be 1000 items in the spreadsheet. Header information can be entered in the Setup screen.



## Update POA&M

The Milestone fields on the POA&M can be updated by clicking the **Update POA&M** button on the MainGui.



## Scan Summary

From the MainGui, click the **Scan Summary** button. A summary of the number of findings for each scan is shown. The original line will show the vulnerability status upon import. The current line will show the current status for each scan. In order for the current line to be correct for any particular scan, the user must first view that scan from the Scan Results Form.



There are two reports available on the Scan Summary Form, a Scan Results Summary Report, which shows the contents of the Scan Summary Form and a Scan Results Report, which shows a report similar to the one on the Scan Results Form. This can be accessed by clicking the View button next to each scan.



## Scan Results

The Scan Results button will become enabled after a Host is selected from the Select Host drop down box. To access a particular host’s scan results, select a host from the MainGui’s “**Select Host**” drop down box and click the **Scan Results** button. The Select Host drop down box can be filtered in various ways. To see only the latest scan for a particular host and checklist, click the “**Click to Show only Latest Scans**” button. It will change to “**Click to** **Show All Scans**”. The Host can also be sorted by selecting one of the radio buttons, Host, STIG, Date or Scan (ID).



### Viewing Vulnerabilities

From the Scan Results Form, details regarding the selected host vulnerabilities can be viewed and updated. Each column header is clickable to toggle between ascending and descending sorting.

The view can also be filtered by the various checkboxes in the Scan Results header section. By checking and unchecking various boxes, results can be filtered based on the checked criteria.

### Updating Vulnerabilities

The object of this form is to provide a status for the compliance of each vulnerability through the development life-cycle. Each vulnerability can be updated with amplifying information. The **Severity** and **Plan** can be changed via drop down combo boxes. The **Severity** cannot be changed unless the corresponding **Plan** has been changed to **Mitigate**.

In order to see the Discussion, Check Content, Fix Text and STIG Comments fields, double click the Description. The STIG comments are specific to each scan, but the Discussion, Check Content and Fix Text fields are the same for all scans for each vulnerability. The **Plan Resolution** field will be filled in with the **STIG Comment** during a STIG import if the existing **Plan Resolution** is blank. Otherwise, it will not be overwritten.



The “Plan Resolution” offers a wholly editable textbox to enter specifics as to the resolution of each particular vulnerability. The contents of the Plan Resolution field will appear in the comments column of the POA&M and RAR. Double clicking inside the Plan Resolution field will bring up an ancillary form that will allow you to enter fields of data associated with the eMASS Risk Assessment Report (RAR). By double clicking the label for Technical Mitigation, stock answers will appear. All data from the form can be cleared by clicking the Clear All Data button. The Baselined check box will show whether a particular vulnerability has been baselined. Baselining should be done from the Setup screen.



In addition, the POA&M can be updated with Milestone information by clicking the **Update POA&M** button on this form or the MainGui. Although not recommended, the **POA&M Status** of a vulnerability can be changed from this form. Only do this if updating the Plan or a subsequent import does not mark the Status correctly. It should be noted that when importing vulnerabilities into eMASS, if the vulnerability already exists and the **Milestone Change** field is not blank, then the **Milestone** in eMASS will be updated.



The **Scan Status** field shows the status of the vulnerability during import. It will never change. Making changes to the **Plan** field will change the **Final Status** field for this scan. The **Plan** field can be changed to **False Positive**, **Mitigate**, **N/A**, **Close** or **Open**. The Final Status will change to **Open**, **Closed** or **N/A**. Changes to the Plan will also make changes to the POA&M Status. The **POA&M Status** can be **Ongoing**, **Completed**, **N/A**, **False Positive**, **Inherited – Ongoing** or **Inherited – Completed**. The **POA&M Status** is automatically marked as Inherited only if ALL the CCIs associated with the vulnerability are marked as Inherited.

Due to RMF requirements, vulnerabilities must be associated with NIST 800-53 Security Controls. Clicking the **Procedure** button brings up a small dialog box from which one or more CCIs/Assessment Procedures can be associated with a particular vulnerability.

**Warning**: If an Open Vulnerability has no Security Control associated with it, the RAR will not show it and the POA&M will show it but with an empty field for Security Control.



**Example of the IA Controls Association Dialog Box**

### Dealing with Vulnerabilities that are Open on one Host and Closed on Another

Changes to the Plan and subsequent imports of matching STIGs for different hosts should (perfection is a goal we can only strive for) mark the **POA&M Status** appropriately. For example, if Windows 10 STIG results are imported for two different Hosts, then if there are any open vulnerabilities on one Host, then the **POA&M Status** should be marked as **Ongoing**. If a vulnerability is **Open** on more than one Host, and a subsequent import closed the vulnerability on one Host, the **POA&M Status** should still be Ongoing. The **POA&M Status** shouldn’t change to **Completed** until the vulnerability is **Closed** for All Hosts.

### Scan Results Report

A report showing the vulnerabilities on the Scan Results Form can be viewed by clicking the **Scan Results Report** button. The vulnerabilities can be filtered by selecting or unselecting the various check boxes on the Scan Results Form. The particulars filtered selected will appear on the upper right hand side of the report.



### Missing Controls

Clicking the **Missing Controls** button will show any vulnerabilities that have no CCI associated with it. Double clicking any vulnerability will move to that record on the form. It may show an associated vulnerability that is not on this particular scan. If that is the case, it is suggested that you utilize this form on the **All Scan Results Form**. There are two reasons that a vulnerability may have no CCI associated with it. First, there may actually be no CCI associated with the vulnerability. Not all STIGs have been updated to include CCIs. Second, there may be a CCI associated with the vulnerability, but it is not selected based on Confidentiality, Integrity or Availability. In addition, when the **Procedure Paint On/Off** is **On**, then the text of the **Procedure** button will show as Red.



### Procedure Paint On/Off

When the **Procedure Paint On/Off** is **On**, then the text of the Procedure button may change color. **Red** for missing CCI, **Blue** for Not Applicable CCI and **Green** for Inherited CCI. While this field is set to On, it repaints the screen constantly, making it annoying.

### Closing the Scan Results Form

The Scan Results Form should always be closed using the **Close** button.

## All Scan Results

The **All Scan Results Form** is similar to the **Scan Results Form** but the results for ALL scans are shown. Certain limitations have been set. The **Plan** field cannot be changed unless the scan is the latest for a particular host and scan type.



### All Scan Results Report

The **All Scan Results Report** will show All Open Findings.

### Click to Show Only Latest Scans

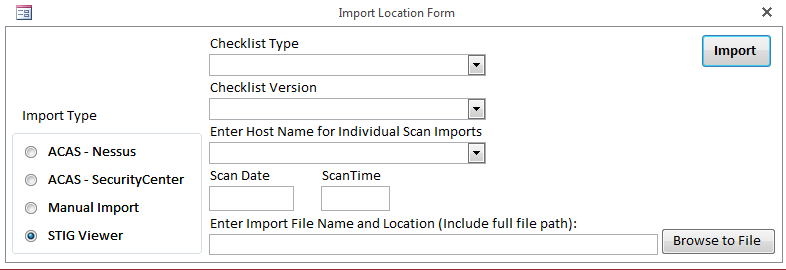
Clicking the **Click to Show Only Latest Scans** button will filter the form to show only the latest for each host and scan.

### Missing Controls

The **Missing Controls** button works the same as on the **Scan Results Form**.

## Import Data

To import scan data into SRP, click the **Import Data** button from the MainGui Form. This launches the Import Location Form.



Radio buttons allow the user to select between five types of import formats: **ACAS - Nessus**, **ACAS – SecurityCenter**, **Manual Import**, **STIG Viewer v.1.2** or **STIG Viewer v.2.X.** The STIG Viewer v.1.2 is still supported because v.2.X does not export the Fix Text field. You need to know the following to import a scan:

* ACAS – Nessus Import
  + From Nessus, select a scan
  + From the Export drop down box, select CSV
  + Save the file



* ACAS – SecurityCenter Import
  + From SecurityCenter, select Scanning 🡪 Scan Results
  + Select a scan
  + Click the Report button
  + Select the Detailed Vulnerability Template
    - The Detailed Vulnerability Template is one of four provided on the DoDs ACAS web site
  + Give the export a name and click the Launch button
    - If the report fails, log out of ACAS, log back in and retry
  + Go to Reporting 🡪 Report Results
  + Select the report and click the Download button
  + Save the file
  + The .csv file will appear in you download directory







* Manual Import – Use Manual Scan Template saved as Excel Spreadsheet, .xlsx
* STIG Viewer Import –
  + From the Export Menu 🡪 Select CSV File (Excel)
  + Make sure all STIG Items and Checklist Items are checked
  + Click File button to select name and location of file
  + Click Save
  + Click Export button (sometimes it is hidden)
  + A CSV file will be generated
  + File name must be no more than 60 characters maximum
  + File name must have no periods other than the one before the extension

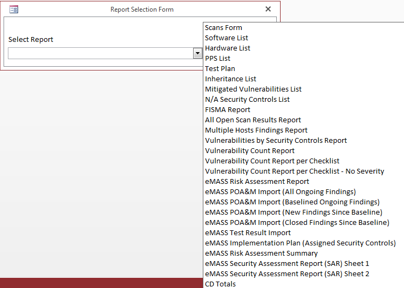
Select the scan data file by clicking the **Browse to File** button and choose the appropriate file (e.g. ManualScans.xlsx). Then click **Open** to continue back to the Import Location Form. From there click the **Done** button. On the Import Location Form, click the Import button.

If the import goes smoothly, a pop-up dialog will appear expressing a successful import.

When the scan data is successfully imported into the SRP database, the Scan Results Form will open, showing the imported scan.

## Forms & Reports

The Forms & Reports button shows a list of Forms, Reports and Queries that provide more information about a scan or package.



### Scans Form

The Scans Form shows all scans along with Date, Time, Host, Scan ID, Checklist Type and Checklist Version.



### Software List

The Software List shows software associated with a system. It can be exported out in a report that can be imported into eMASS.



### Hardware List

The Hardware List shows hardware associated with a system. It can be exported out in a report that can be imported into eMASS.



### PPS List

The PPS List shows ports, protocols and services associated with a system. It can be exported out in a report that can be imported into eMASS.



### Test Plan

The Test Plan shows the scans done for a system. It can also show the findings for each scan.



### Inheritance List

The Inheritance List shows all Security Controls listed as Inherited.



### Mitigated Vulnerabilities List

The Mitigated Vulnerabilities List shows all vulnerabilities that have had their **Severity** changed.



### N/A Security Controls List

The N/A Security Controls List shows all Security Controls that are marked as Not Applicable along with the Not Applicable Justification.



### FISMA Report

The FISMA Report shows an annual FISMA Report with some fields already filled in.



### All Open Scans Results Report

The All Open Scans Results Report shows ALL Open vulnerabilities.



### Multiple Hosts Findings Report

The Multiple Hosts Findings Reports shows findings across multiple hosts. Select Open, Closed or N/A findings.





### Vulnerabilities by Security Controls Report

The Vulnerabilities by Security Controls Report shows a listing of all vulnerabilities and the associated Security Controls, Assessment Procedures and CCIs. First select Open, Closed and/or N/A.





### Vulnerability Count Report

The Vulnerability Count Report shows the count of all vulnerabilities by status.



### Vulnerability Count Report per Checklist

The Vulnerability Count Report per Checklist shows the count of all vulnerabilities by status, severity and checklist type.



### Vulnerability Count Report per Checklist – No Severity

The Vulnerability Count Report per Checklist – No Severity shows the count of all vulnerabilities by status and checklist.



### eMASS Risk Assessment Report (RAR)

The RAR is exportable in the format expected for the RAR template.

### eMASS POA&M Import (All Ongoing Findings)

The eMASS POA&M Import (All Ongoing Findings) is in the format expected for the eMASS POA&M Import Template. This report shows all open findings.

### eMASS POA&M Import (Baselined Ongoing Findings)

The eMASS POA&M Import (Baselined Ongoing Findings) is in the format expected for the eMASS POA&M Import Template. This report shows only open findings that have been baselined.

### eMASS POA&M Import (New Findings Since Baseline)

The eMASS POA&M Import (New Findings Since Baseline) is in the format expected for the eMASS POA&M Import Template. This report shows only open findings that have not been baselined.

### eMASS POA&M Import (Closed Findings Since Baseline)

The eMASS POA&M Import (Closed Findings Since Baseline) is in the format expected for the eMASS POA&M Import Template. This report shows only closed findings that were marked as baselined. These findings would be marked as Closed in eMASS.

### eMASS Test Result Import

The eMASS Test Result Import is in the format expected for the eMASS Test Result Import Template. This report shows the compliance status of all CCIs.

### eMASS Implementation Plan (Assigned Security Controls)

The eMASS Implementation Plan (Assigned Security Controls) shows the implementation status of all assigned Security Controls.



### eMASS Risk Assessment Summary

The eMASS Risk Assessment Summary shows Risk Assessment Summary of all assigned Security Controls.



### eMASS Security Assessment Report (SAR) Sheet 1

The eMASS Security Assessment Report (SAR) Sheet 1 shows the information for the first sheet of the SAR for import into the DoD SAR template.

### eMASS Security Assessment Report (SAR) Sheet 2

The eMASS Security Assessment Report (SAR) Sheet 2 shows the information for the first sheet of the SAR for import into the DoD SAR template.

### CD Totals

The CD Totals shows the count of findings as listed in the Certification Determination completed by the SCA representative.



# Troubleshooting

## Windows 7

If an Update Fail error occurs when opening the database for the first time, do the following:

1. Open the front end Scan Results Database while holding Shift key
2. Click Linked Table Manager from the External Data menu
3. Check the Always prompt for new location check box
4. Click Select All
5. Click OK
6. Select the Location of your back end database
7. Click Open
8. Click OK on the pop up dialog box
9. Click Close on the Linked Table Manager
10. Close the database
11. Reopen the database

If the splash screen appears with a Security Warning behind it, do the following:

1. Click Enable Content on the Security Warning
2. Close the Splash Screen
3. Click Setup on the MainGui
4. Click the Relink Database button
5. Follow steps 3 through 11 above

\*\*Note: Sometimes it may be necessary to place the database location in the list of “Trusted Locations”. From the options menu, click Trust Center then the Trust Center Settings button. Click Trusted Locations then Add New Locations.

## Microsoft Office 2007

If you are trying to open the database with Microsoft Office 2007 and are encountering issues, do the following:

1. Create a new blank Access database
2. Delete the default table
3. Click External Data 🡪 Import & Link 🡪 Access
4. Browse to the front end database (the one without the “be” in it)
5. Select Import tables, etc.
6. Click Ok
7. For each of the tabs on the Import Objects box, click Select All
8. Then click OK
9. When complete, Go to File 🡪 Options 🡪 Current Database 🡪 Display Form and enter frm\_Splash
10. Make sure that Overlapping Windows is selected in Document Window Options
11. Optionally enter an Application Title to appear on the title bar of the database.

## Verify data is correct

When importing data, verify that the import data is correct.

## Compact and Repair

Compact and Repair the database routinely. Compact the back end database separately from the front end database only when the front end database is closed.

## Changing Data Issues

In order to prevent problems, make sure that when you change data, you click on or go to another record before attempting to close a form or click any buttons.

## Database goes to code window when opening for the first time.

This may be the result of a missing reference. Click the square stop button. Click Tools 🡪 References. If one of the references listed shows the text, Missing, uncheck it. You may have to close and reopen the database to get to the References.

# Point of Contact

Technical Point of Contact:

Robert Sakey

858-826-9243

robert.m.sakey@saic.com

# Revision History

The Revision History is a list of the changes made to each successive version of the Scan Results Processor. This manual is updated for each version.

## 1.0.0

* Initial Version

## 1.0.1

* Changed labels of Vulnerability and Non-Vulnerability fields to Non-Compliant Results and Compliant Results.
* Added ability to copy Actual Results field to Compliant Results field by double clicking on Actual Results label in Assessment Procedures Form.
* Removed Expected Results from Assessment Procedures Form.
* Added instructions text to Test By label on Assessment Procedures Form.
* Changed DoD Tier 1 Partial/Complete Inheritance text in Security Controls to DoD Tier 1 Hybrid/Common Control.

## 1.1.0

* Fixed query for Add Vulnerability to 800.53 Scan Results
* Updated buttons and Reports for Security Controls and Assessment Procedures and other forms
* Added double click functionality to FISMA Report Date field
* Added CyberSafe A and CyberSafe B to Overlay field on SAR
* Moved Classified Overlay to beginning of section 6 of SAR
* Updated truncated CCI Definition and Implementation Guidance Text
* Created RAR Sheet 1 that can be exported to RAR template and added as new sheet with sheet name the same as query name
* Disabled Inherited From field on Assessment Procedures form if CCI cannot be inherited
* Updated Assessment Procedures and Security Controls with DON Tier 2 Inheritance
* Added IAVM functionality
* Added Assessment Procedures view when clicking Security Control on Security Control Form
* Fixed Database open to default to Splash form

## 1.2.0

* Added Export to PDF button on Security Controls and Assessment Procedures Forms
* Added Export to Excel button on Security Controls and Assessment Procedures Forms
* Adjusted Double Click functionality on Assessment Procedures Form
* Added Tier 3 Inheritance
* Added ability to see if Overlays have been added by the color of the Overlay buttons on the Overlays form

## 1.2.1

* Added IAVM tables and Overlay fields to list of deleted items when clearing database
* Error checking applied to opening and closing forms
* Changed Import Location Form to automatically check for the STIG Viewer version

## 1.2.2

* Fixed Navigation Pane opening when importing STIG
* Fixed setting of Final Scan options when closing Scan Results Form
* Fixed sort on Scan Results Form and All Scan Results Form
* Fixed setting Plan when creating vulnerability from Assessment Procedures
* Fixed setting POAMStatus when creating vulnerability from Assessment Procedures
* AutoBackup added to Setup screen to allow for an auto backup of backend database when importing scans
* Added ability to filter for Applicable IAVMs on IAVM Project Report
* Fixed bug causing Navigation Pane to open when importing scans
* Added CVE field from ACAS SecurityCenter scans to Check Content field