APPENDIX B: FEMA 452: Risk Assessment Database© V3.0 User Guide

TABLE OF CONTENTS

Any opinions, findings, conclusions, or recommendations expressed in this publication and application do not necessarily reflect the views of FEMA. Additionally, neither FEMA or any of its employees makes any warrantee, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process included in this publication and application. Users of information from this publication and application assume all liability arising from such use.

Introduction

To support the facility assessment process, this easy to use Risk Assessment Database application is provided with FEMA 452, Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings. The Risk Assessment Database is a standalone application that is both a data collection tool and a data management tool. Assessors can use the tool to assist in the systematic collection, storage and reporting of assessment data. It has functions, folders and displays to import and display threat matrices, digital photos, cost data, site plans, floor plans, emergency plans, and certain GIS products as part of the record of assessment. Managers can use the application to store, search and analyze data collected from multiple assessments, and then print a variety of reports.

The first task is to download and install the database program from the FEMA website. Follow the download and self installation instructions. It is recommended to install the database on two separate systems: one to use as the Master Database and one to use as a temporary Assessment tool.

Install one copy of the program as the Master Database on a computer at your organization's headquarters. This will act as the permanent database that stores assessments, produces reports, and is used to manage the assessment program. This is installed one time and is the permanent program. This database is normally run in the Master Database operating mode. For small organizations, the Master Database can also be used to perform the Assessment Tool functions and directly collect assessment data. Note: be sure to change the initial generic passwords.

Install a second copy of the program to use in the Assessment Tool operating mode on the computer(s) that your assessors will use to collect data, such as a laptop. This is intended to be a temporary database that can be used to collect data, pass the collected data on to the Master Database, and than have its records deleted so it can be used for other assessments. This database is normally run in the Assessment Tool operating mode. Note: be sure to change the initial generic passwords.

When an organization wants to conduct an assessment of a facility or a series of facilities, it uses the database in the Assessment Tool operating mode. Pre-assessment tasks are preformed and information is collected and loaded into the blank temporary Assessment Tool program. Into this Assessment Tool is placed references, site plans, GIS portfolios, and other facility specific data that is known about the assessment facility or is developed during the pre-assessment phase. Loading this information can be done by a Project Manager before the assessment or by an assessor during the assessment.

The assessment team then conducts the assessment and records information using the Assessment Tool operating mode on one or more computers (usually laptop computers). At the end of the assessment, the assessment team uses the Import Checklist function in the Assessment Tool operating mode to combine their checklist, vulnerability and

recommendation entries. They also manually combine photos, and miscellaneous files into the lead assessor's database folder. The Project Manager then uses the Import Assessor Database function in the Master Database operating mode to transfer the complete assessment data and files into the Master Database for analysis and printing.

After initially installing the application and changing the generic passwords, access to that Risk Assessment Database becomes restricted to only those designated users who have been assigned permission by their administrator. Also, data may be viewed by authorized users of the database, but changes to the data may only be made by those granted permission. All access permission questions should be directed towards the database Administrator of your organization.

The following are the hardware and software requirements for the Risk Assessment Database:

Pentium® 4 or equivalent processor
Windows XP®
MS Access® 2002
256 MB of RAM recommended for all components

Security: The Database must be opened using the shortcut installed during the initial setup. The initial passwords are:

Name: Administrator	**Password**: Administrator
Name: Assessor	**Password**: Assessor
Name: Editor	**Password**: Editor
Name: Reader	**Password**: Reader

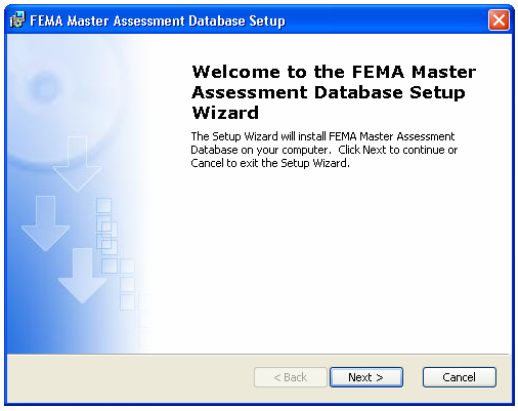
It is recommended that your database administrator assign new user names or change these passwords following the initial installation of the database. See the Database Administrator Information section and the Change Password section of the User Guide for more detailed information.

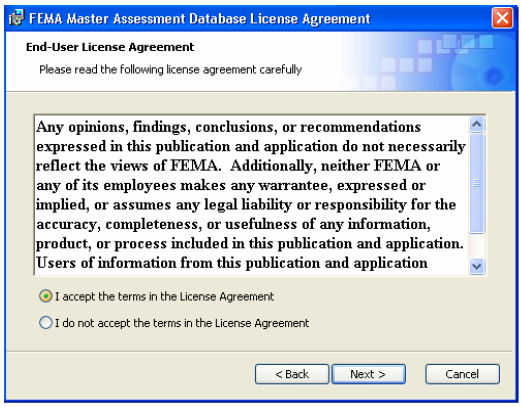
Installation Process

- Install one copy of the program as the Master Database on a computer at your organization's headquarters. Begin the installation process by left clicking on the SETUP.EXE for the Master Database. The normal way to install a program is to close all other programs, then left click <Start>, <Run>, identify the location where the SETUP.EXE program can be found (CD, C:/Temp, or some other storage location on hard drive or media).

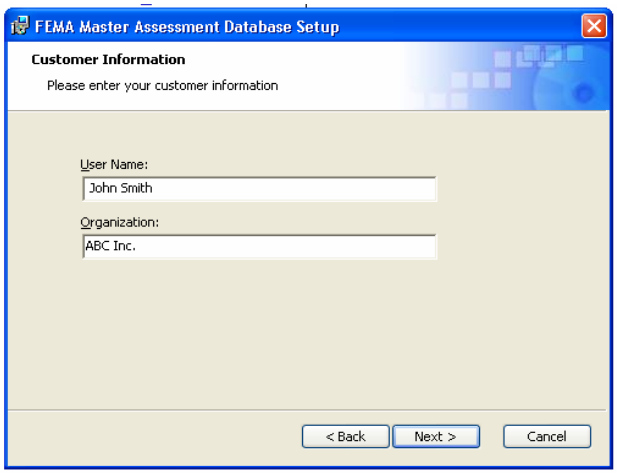
- The Install Wizard first identifies the name of the software being installed. Left click <Next> to continue after confirming that this is the software you want to install.

- A standard screen showing the End User License Agreement will appear. Read as you feel appropriate, then left click on the <Accept> circle, and left click on <Next> to continue with the installation.



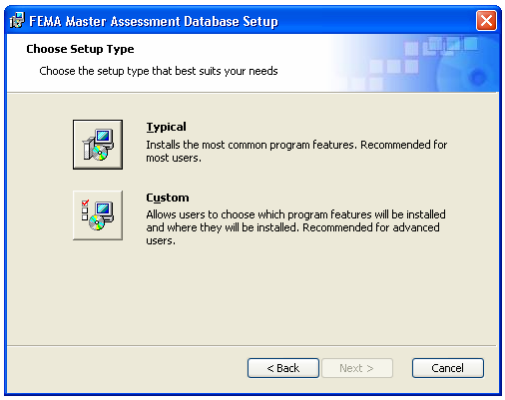


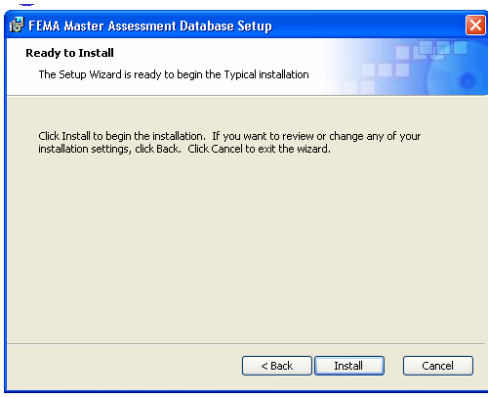
- Add the User Name and Organization in the appropriate windows. Continue with the installation by left clicking <Next>.



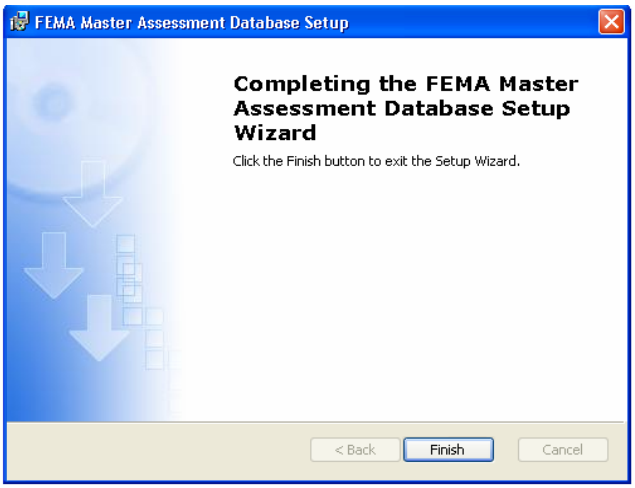
- There is no advantage in using the Custom Installation. There are no component programs to select. The only feature that the Custom Installation allows is to change the file name and/or file location. In most cases you should follow the Typical Installation. To proceed, left click on <Typical>.

- A standard screen to ensure you are ready to install will appear. Proceed by left clicking <Install>.





- If the Access program is not located in the standard location, the Install Wizard will take a long time looking for it with a searching flashlight. It should eventually find it and get to this screen. The final standard screen indicates the Install Wizard has completed the installation. Left click <Finish> to end the installation.

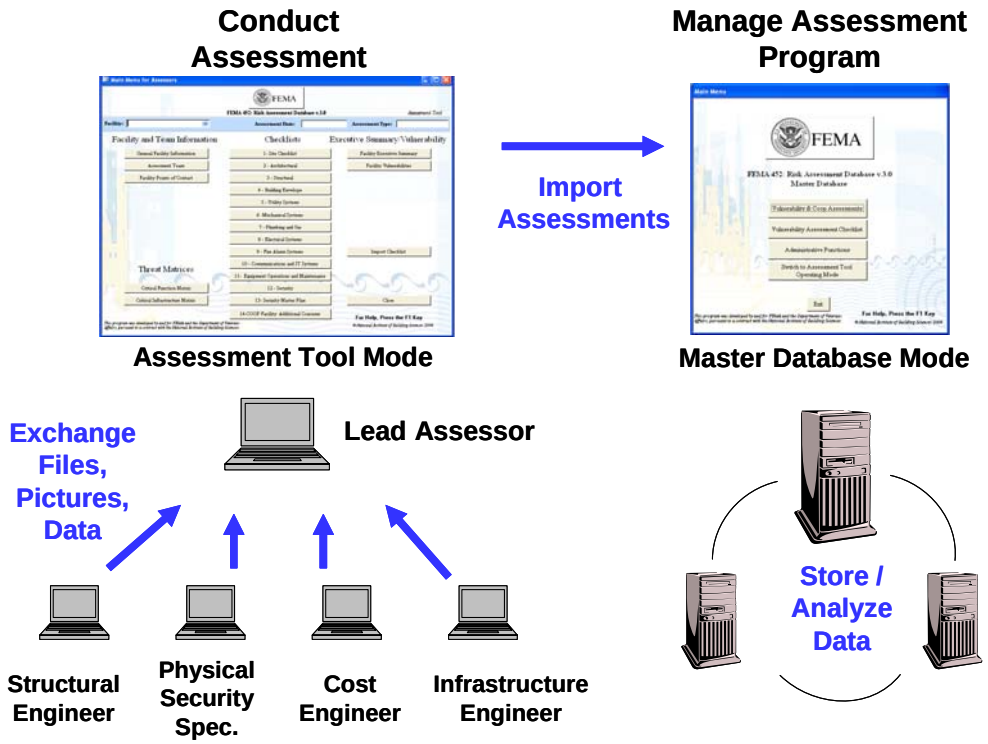


Following the same procedure, install a second copy of the program to use in the Assessment Tool operating mode on the computer(s) that your assessors will use to collect data, such as a laptop.

Use of the Database

The first thing to understand is that an organization will generally use two different copies of the database: one loaded on a laptop and operating in the Assessment Tool mode for conducting assessments in the field, and the other loaded on a computer at your organization's headquarters and operating in the Master Database mode for collecting the results from the assessors, printing reports**,** and archiving the results from a number of assessments. The Master Database copy also provides the organization the ability to search for vulnerabilities common to many assessed facilities, search for specific vulnerabilities, etc. Essentially it can be used as a Risk Management tool to identify and track mitigation measures to reduce risk.

The Assessment Tool mode was designed for engineers and security specialists to be able to easily collect data from the facility being assessed. As you will see, the software is very user friendly. The Master Database mode was designed for the Program Manager.

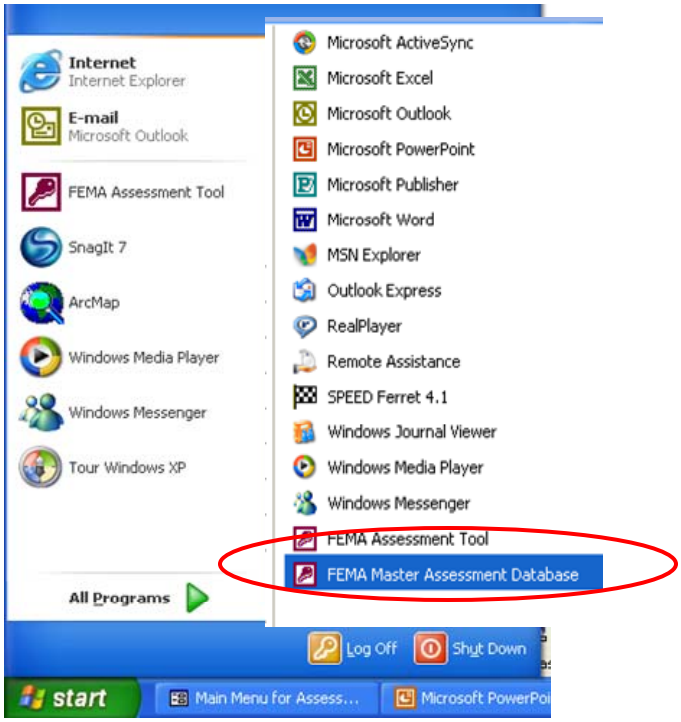


This diagram shows how the two copies of the database interact. When an organization collects information and prepares to conduct an assessment of a facility or a series of facility, a temporary Assessment Tool program is prepared. Into this Assessment Tool is placed references, site plans, GIS portfolios, and other facility specific data that is known about the assessment facility or is developed during the pre-assessment phase. Loading this information can be done by a Project Manager before the assessment or by an assessor during the assessment.

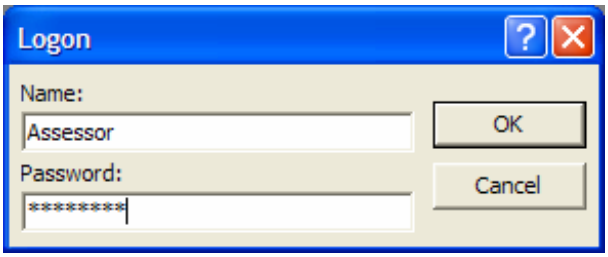
This Assessment Tool is then given to the assessment team and is loaded on one or more assessment computers (usually laptop computers). The assessment team then conducts the assessment and records information using the Assessor Tool operating mode. At the end of the assessment, the assessment team leader uses the Import Checklist function in the Assessment Tool operating mode to combine the team's checklist, vulnerability and recommendation entries into one record. They also manually combine photos, and miscellaneous files into the lead assessor's database folder. The Project Manager then uses the Import Assessor Database function in the Master Database operating mode to transfer the complete assessment data and files into the Master Database for analysis and printing.

Opening the Database

- To open the Master Assessment Database, you first left click on <Start>, then <Programs>, and look for the <FEMA Master Assessment Database> to left click. The FEMA Master Assessment Database should be at the end of the Startup Program Menu immediately after the installation. You can move the buttons for the FEMA Master Assessment Database to another location within the Startup Menu at any time.



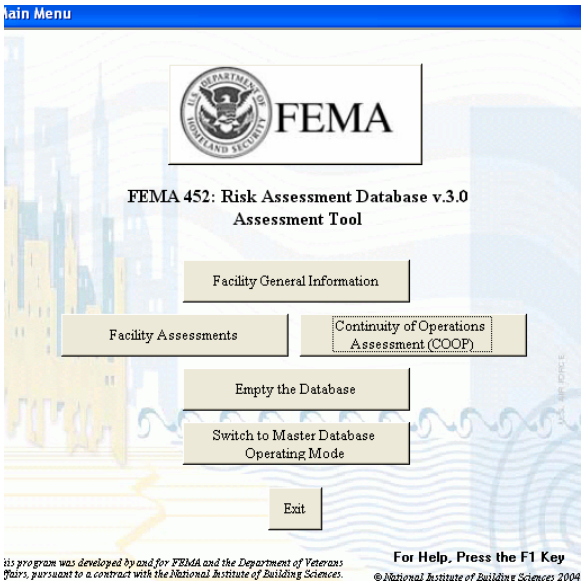
- The first action to enter the database is the Logon. You can enter the database Tool as an Assessor, Editor, Reader or Administrator. The initial Password for Assessor is “Assessor”. A Database Manager / Administrator is needed to change the Logon Names and Passwords.



- This leads to a Main Menu of the database. It may start in either in the Assessment operating mode or in the Master Database operating mode. (It opens in the mode for which it was last used.)

Assessment Tool Operating Mode

- The first action is to identify the facility assessment in the Assessment Tool by left clicking on < Facility General Information> and creating a new assessment. Any assessor can create an assessment in the Assessment Tool.



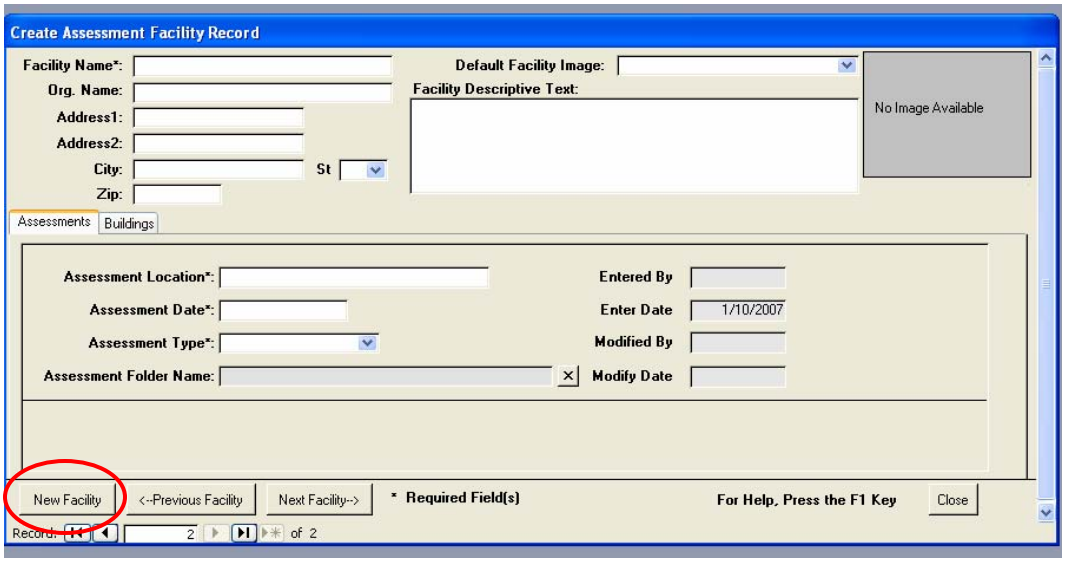
- If the Facility Information has already been loaded, you can go directly to an assessment screen by left clicking on <Facility Assessments> or <Continuity of Operations Assessments (COOP).

- Assessor laptops have limited storage capacity and can become bogged down by continuing to store many assessments. The <Empty Database> feature allows clearing of the database (with multiple requests for confirmation). Copy the database and all other collected information to a CD before emptying, as assessors may find it beneficial to refer to similar entries from previous assessments, especially recommended mitigation measures for similar vulnerabilities. Note: <Empty Database> cleans Facility Information, Team Members, Points of Contact, Observations, Recommendations, Vulnerabilities, Status, Costs, and the Executive Summary for ALL facilities in the Assessment Tool database. However, it does NOT empty the GIS Portfolio, Miscellaneous Files, and Photos in their separate subfolders, as these are not part of the Microsoft Access database. Thus, these files have to be deleted separately.

- The <Switch Operating Modes> tab takes you to the Master Database mode. This enables the user to manage collected information. It also enables an assessor to use the reports feature to check the final look of the information entered, to prevent duplicate entries, and to easily review the information rather than having to scroll through the database.

Create Assessment

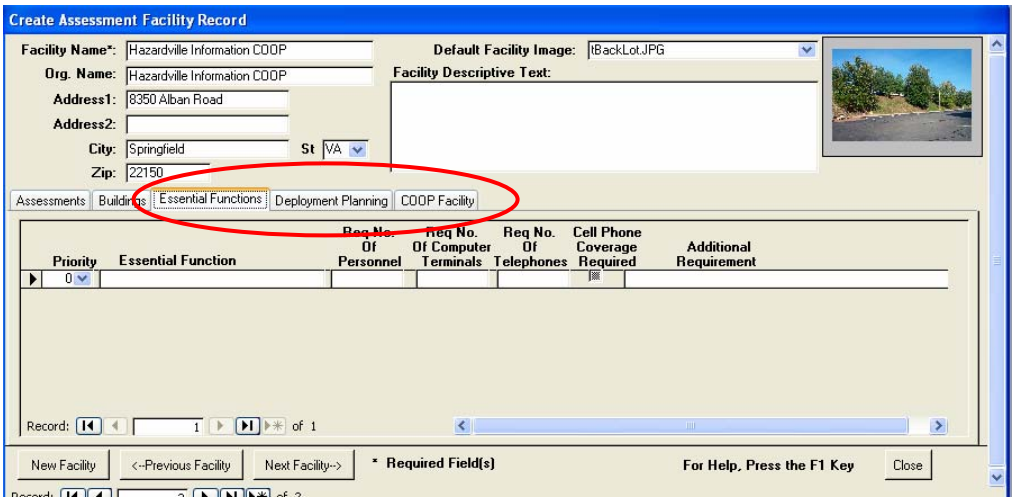
The first time you enter the database (with no prior assessments entered), click <Facility General Information> and the software will immediately go to the <Create Assessment > input screen. If assessments have already been entered, then a new assessment can be created by left clicking on the <New Facility> button in the lower left corner.



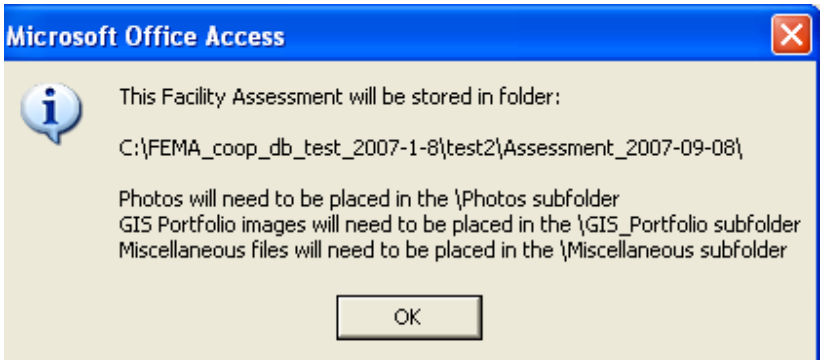
Note the asterisked (*) entries that are the minimum required to create an assessment: Facility Name, Assessment Location, Assessment Date, and Assessment Type. Facility Name, Assessment Location, and Assessment Date are self explanatory. However, Assessment Type needs some clarification.

For Facility Assessments, select from the drop down box “Facility Tier 1”, “Facility Tier 2”, or “Facility Tier 3”. Refer to FEMA 452, Page 3-2, for information on Assessment Type / Level of Assessment.

For COOP Assessments, select “COOP Assessment”. This will prompt the system to display Checklist #14 on the Assessment Tool main menu and also add the following three tabs to this form: Essential Functions, Deployment Planning and COOP Facility. Use these three tabs to record COOP related information on the facility.



When you create the facility, the software automatically creates subfolders named GIS Portfolio, Miscellaneous Files, and Photos, all under a main folder that uses the assessment location and assessment date as the main folder name. If you changed the program location using Custom Installation, then you should make note of the file path that these subfolders are placed in, as you will need that information to properly load and link the contents of these subfolders to the Assessment Tool database.
Left click <OK> to finish creating the Assessment.



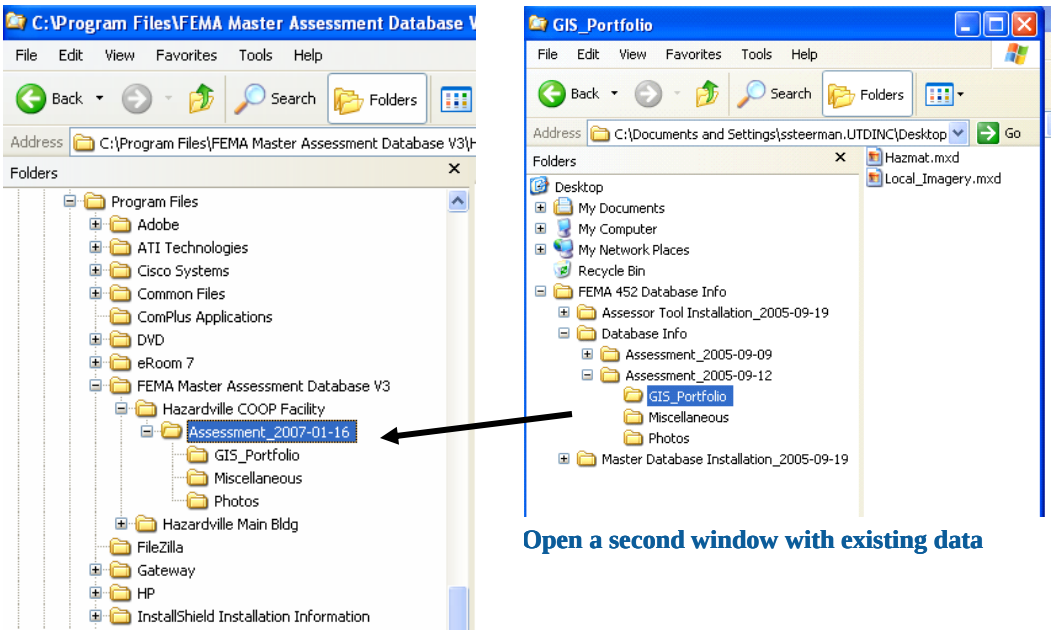
Load Information Into the Newly Created Assessment Subfolders

- First open My Computer or Windows Explorer to find the storage locations created by the Assessment Facility creation process.

- Next, open another window in My Computer or Windows Explorer to find the information collected either before or during the assessment.

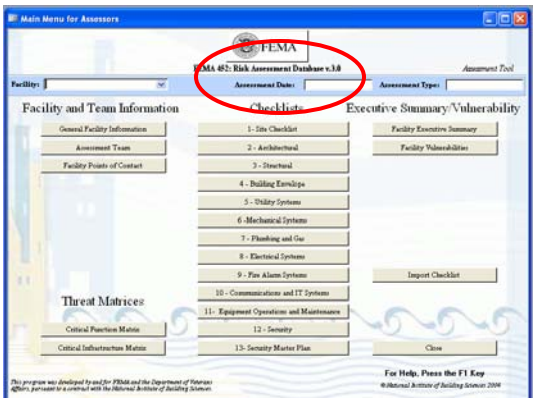
- Conduct a drag-and-drop operation to transfer the files to the necessary subfolders to later link with the database. You can also <Right Click> on the collected files, copy them by left clicking <Copy> in the pull-down menu, and then move to the necessary subfolders, <Right Click> on the appropriate folder, then paste by left clicking <Paste> in the pull down menu. Ensure that all files are transferred – either copied or moved into the necessary subfolder.

- The drag-and-drop operation between the two windows allows transfer of GIS Images, Miscellaneous Files and Photos.

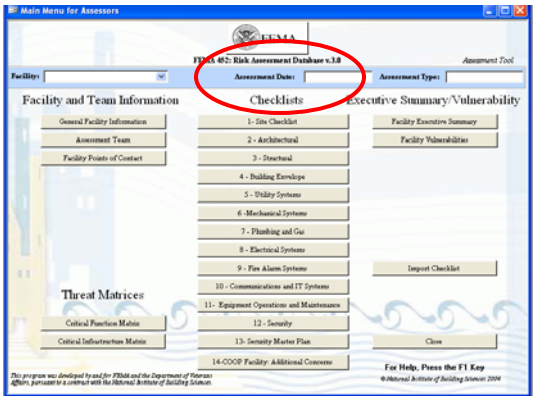


Open a second window with existing data

Main Menu for Assessors



Facility Assessments



COOP Assessments

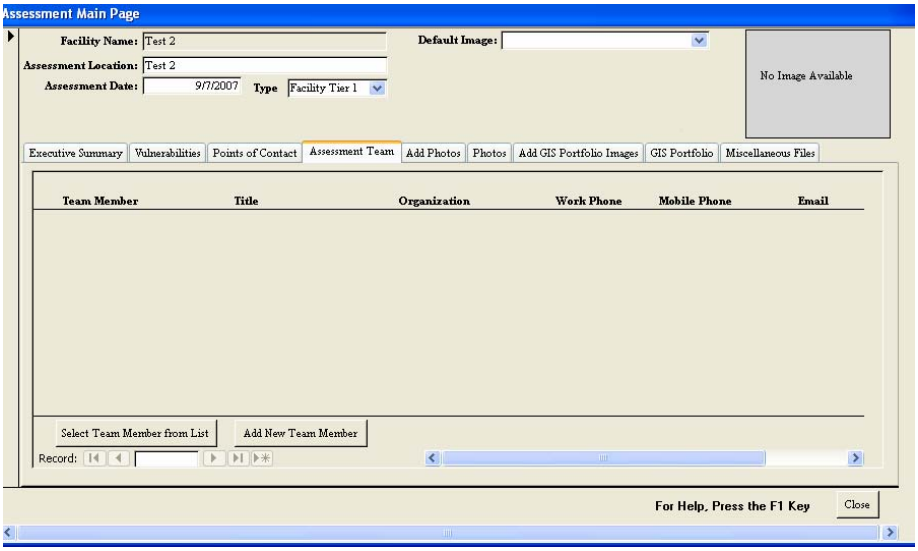
From the Assessment Tool Main Menu, left click on <Facility Assessments> or <Continuity of Operations Assessment (COOP)> to enter the Main Menu for Assessors. This will bring you to the Main Menu for Assessors. The link to <Facility Assessments> provides access to Facility Tier 1 to Facility Tier 3 assessments and the standard 13 checklists. The <Continuity of Operations Assessment (COOP)> link provides access to COOP assessments, the standard 13 checklists and a 14th checklist titled "COOP Facility: Additional concerns". Both forms function in the same manner.

The first action on either screen is to choose an assessment facility, since several may be loaded. This is done using the pull-down list in the "Facility:" window in the top left corner.

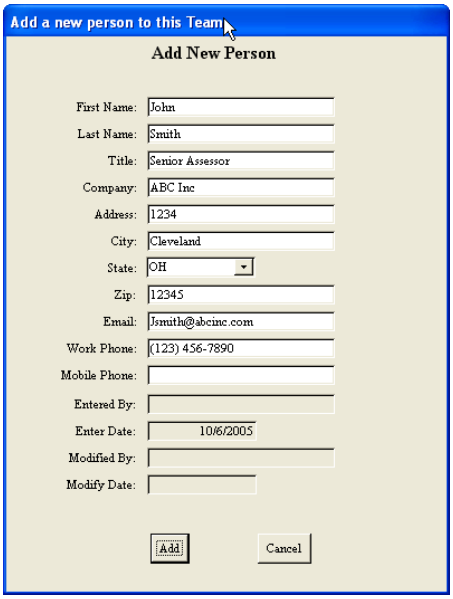
The list will show the names of the facilities that have been created. Once an assessment facility has been chosen, the assessor can go into any of the data entry areas: General Facility Information, Assessment Team, Facility Points of Contact, Threat Matrices, Checklists, Executive Summary or Facility Vulnerabilities.

Assessment Team

The Assessment Team tab takes the assessor to fill-in-the-blank lists for keeping track of team members. Fill in this screen with as much information as is available or desired.



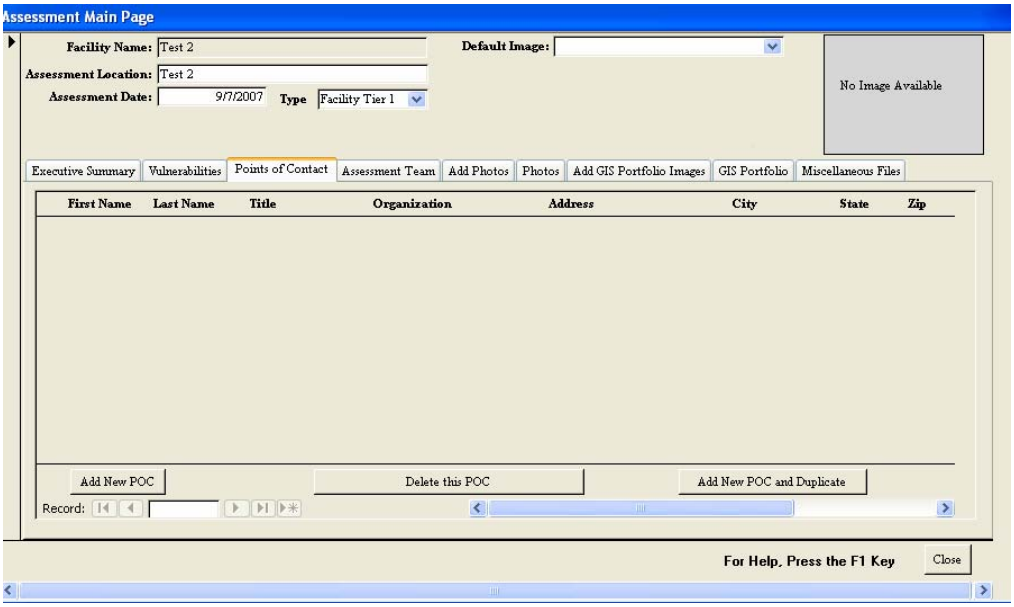
After adding a team member, you are taken back to the Team Members List and you can see the information that was entered. Use the slide scale or keyboard arrows to see the off-screen information. The other buttons allow you to select the Team Member from a List previously generated from other assessments or remove the Team Member from this assessment (Undo Team Member Record).



At this point you can <Close> to go back to the Main Menu for Assessors screen or you can continue loading information for additional team members.

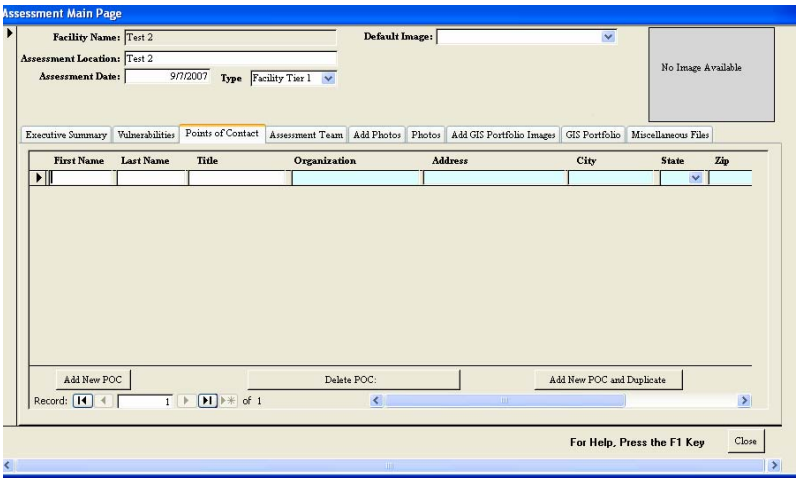
Points of Contact

The Points of Contact tab takes the assessor to the Points of Contact screen for keeping track of the people identified to be contacted during the assessment or that are met during the assessment. The buttons across the bottom allow you to add or delete Points of Contact as needed. Add a POC by left clicking on <Add New POC>.



This input screen is different than the Team Members input screen, as you enter the information directly in each cell. You can enter the information and move to the next cell by using the <Tab> on the keyboard or by left clicking on the cell. Use the slide scale or keyboard arrows to move the screen to see the remaining information on the POC line.

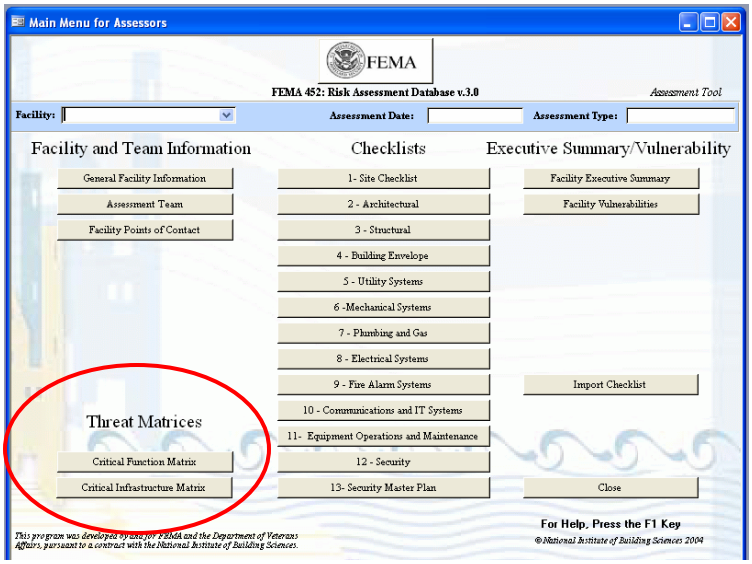
You must press <Enter> or the <Tab> key after the cells are complete to add the information to the database.



There’s even a feature in the POC list to duplicate the address from previous entries, since it is likely that many POCs will have the same business address. Just left click the left column to get the black arrow to appear on the entry with the address to be copied. Then by left clicking on the tab <Add New POC and Duplicate> the light blue address blocks will be duplicated on the next entry line.

Threat Matrices Process

After the available preliminary information is loaded, you can work the Threat Matrices for Critical Functions and Critical Infrastructure. To get to these screens choose an assessment facility and left click either the <Critical Functions Matrix> or the <Critical Infrastructure Matrix> button from the Main Menu for Assessors.



Critical Function Matrix

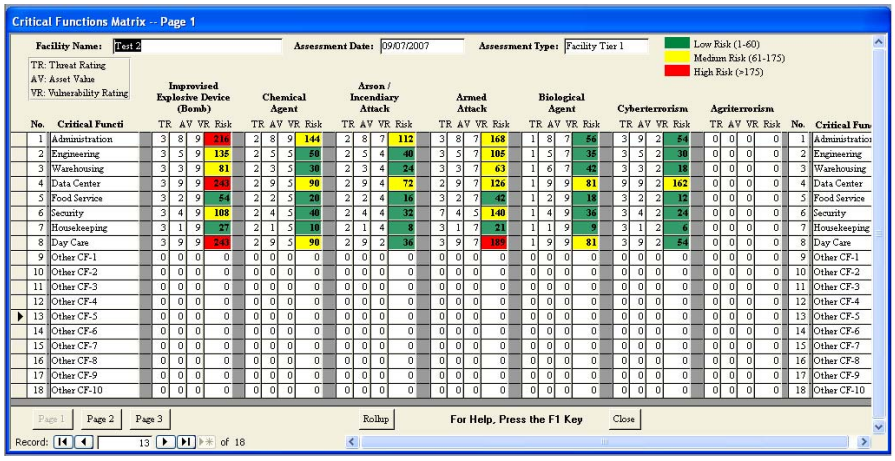
Selecting the <Critical Function Matrix> button will display this screen. Listed are a range of established threats and functions. The matrix allows entry of Threat Rating, Asset Value, and Vulnerability Rating following the 1 to 10 scale as listed in FEMA 452. The Risk Rating is then automatically computed and color coded according to the established scale.

To maintain the FEMA 452 process, the basic Threats and Functions can not be renamed. However, there are unassigned placeholders that can be used to record an organization's unique Critical Functions and Threats. The placeholders for functions are listed under the Critical Function column as "Other CF-1" to "Other CF-10". The threat placeholders are listed across the top of the matrix as "Other 1" and "Other 2". Organizations can designate a meaning for a placeholder, use the placeholder to collect data, then after exporting the matrix to Microsoft Excel©, change the name of the placeholder to a specific threats or function.

- Selecting the <Page 2> or <Page 3> buttons will display additional Threats / Hazards.
- Selecting the <Rollup> button displays a consolidated Functions matrix.

Threats →

Function ↓



Asset Value	**1- 10**		**Low risk (1-60)**
Threat Rating	**1- 10**		**Medium risk (61-175)**
Vulnerability Rating	**1- 10**		**High risk (> 175)**

Critical Infrastructure Matrix

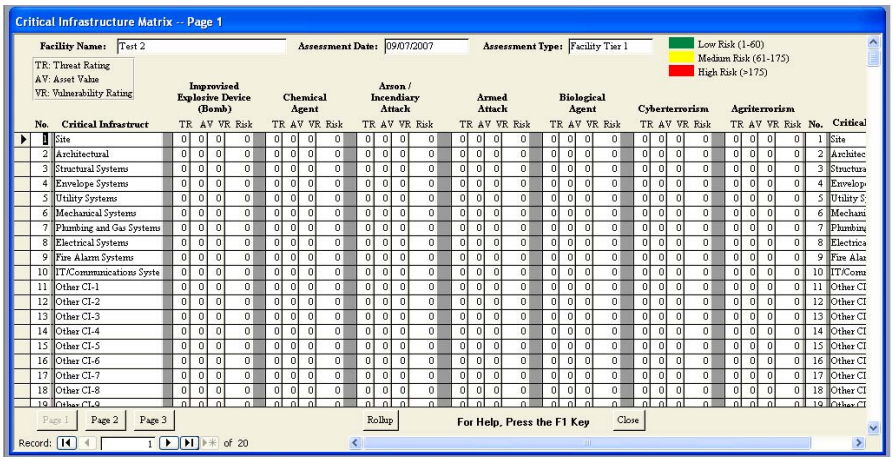
Selecting the <Critical Infrastructure Matrix> button will display this screen. Listed are a range of established threats and functions. The matrix allows entry of Threat Rating, Asset Value, and Vulnerability Rating following the 1 to 10 scale as listed in FEMA 452. The Risk Rating is then automatically computed and color coded according to the established scale.

To maintain the FEMA 452 process, the basic Threats and Infrastructures can not be renamed. However, there are unassigned placeholders that can be used to record an organization's unique Critical Infrastructures and Threats. The placeholders for Infrastructure are listed under the Critical Infrastructure column as "Other CI-1" to "Other CI-10". The threat placeholders are listed across the top of the matrix as "Other 1" and "Other 2". Organizations can designate a meaning for a placeholder, use the placeholder to collect data, then after exporting the matrix to Microsoft Excel©, change the name of the placeholder to a specific threat or Infrastructure.

- Selecting the <Page 2> or <Page 3> buttons will display additional Threats / Hazards.
- Selecting the <Rollup> button displays a consolidated Infrastructure matrix.

Threats →

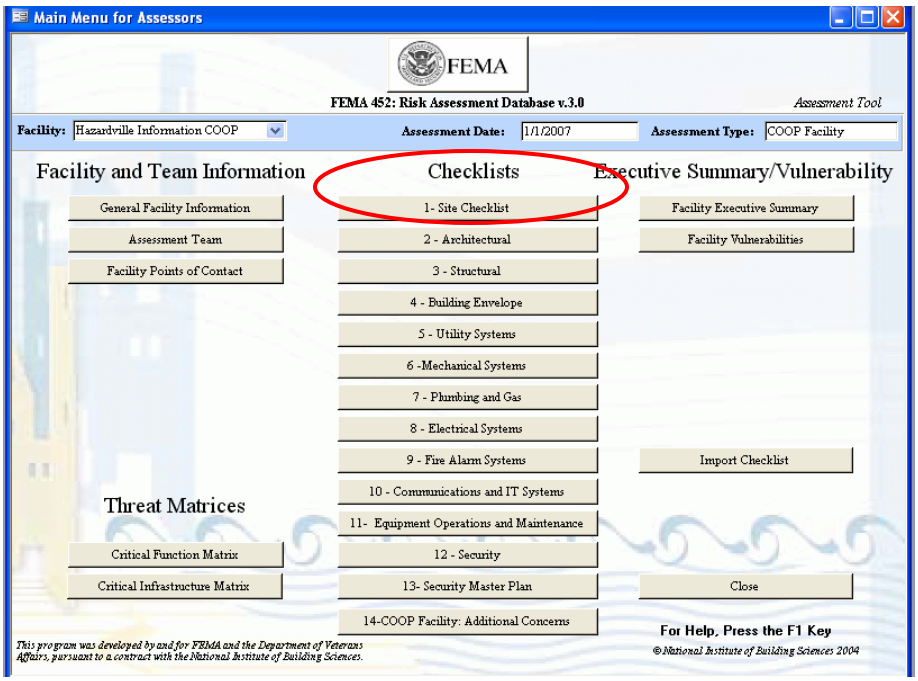
Infrastructure ↓



Asset Value	**1- 10**		**Low risk (1-60)**
Threat Rating	**1- 10**		**Medium risk (61-175)**
Vulnerability Rating	**1- 10**		**High risk (> 175)**

Checklist Process

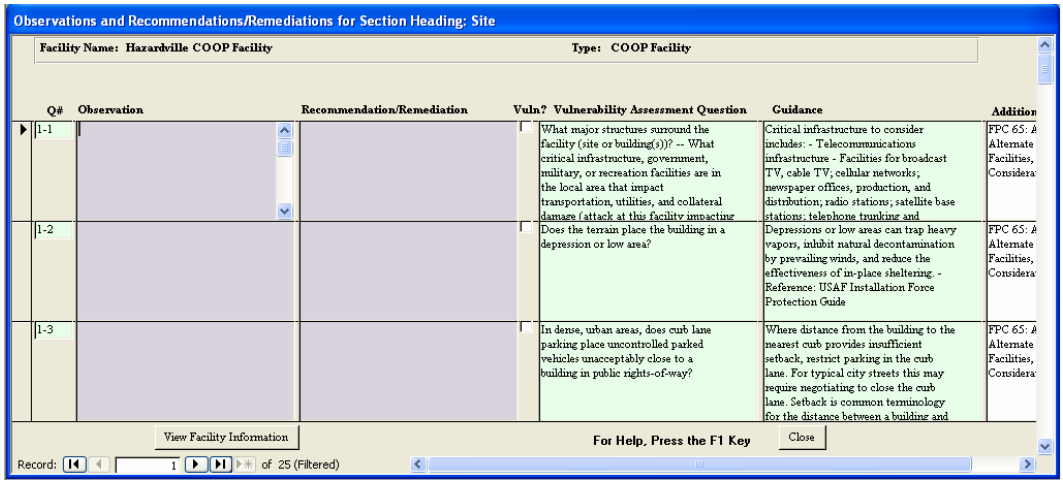
The standard 13 checklists and the 14th checklist titled "COOP Facility: Additional concerns", run down the middle of the Main Menu for Assessors screen. After selecting an assessment facility, left clicking on a checklist, the <1 – Site Checklist> as an example, brings up the format of all checklists within the Assessment Tool.



Assessment Checklists

The format of the Site Checklist is like all the other checklists.

- The first column contains an arrow to indicate which row is selected for data entry.
- The second column on the left is the checklist question number [Section Number – Question Number]
- The third column is the Observation made during the assessment. This could describe a vulnerability identified by the assessor.
- The fourth column is the Recommendation / Remediation made by the assessor to mitigate concerns with this question and observation.
- The fifth column is reserved for identifying the questions which have an observation identified as a vulnerability.
- The sixth column is the question itself, taken right from the FEMA 426 Building Vulnerability Assessment Checklist.
- The seventh column is the guidance associated with that question, also found in the FEMA 426 Building Vulnerability Assessment Checklist.
- The eighth column is a cross reference to COOP related guidance.



If an Observation was identified by the assessor as a vulnerability to consider, he places a check mark in the "Vuln?" box by putting the pointer on the box and left clicking. This copies the Observation (now a Vulnerability) and the Recommendation / Remediation to the Facility Vulnerability list.

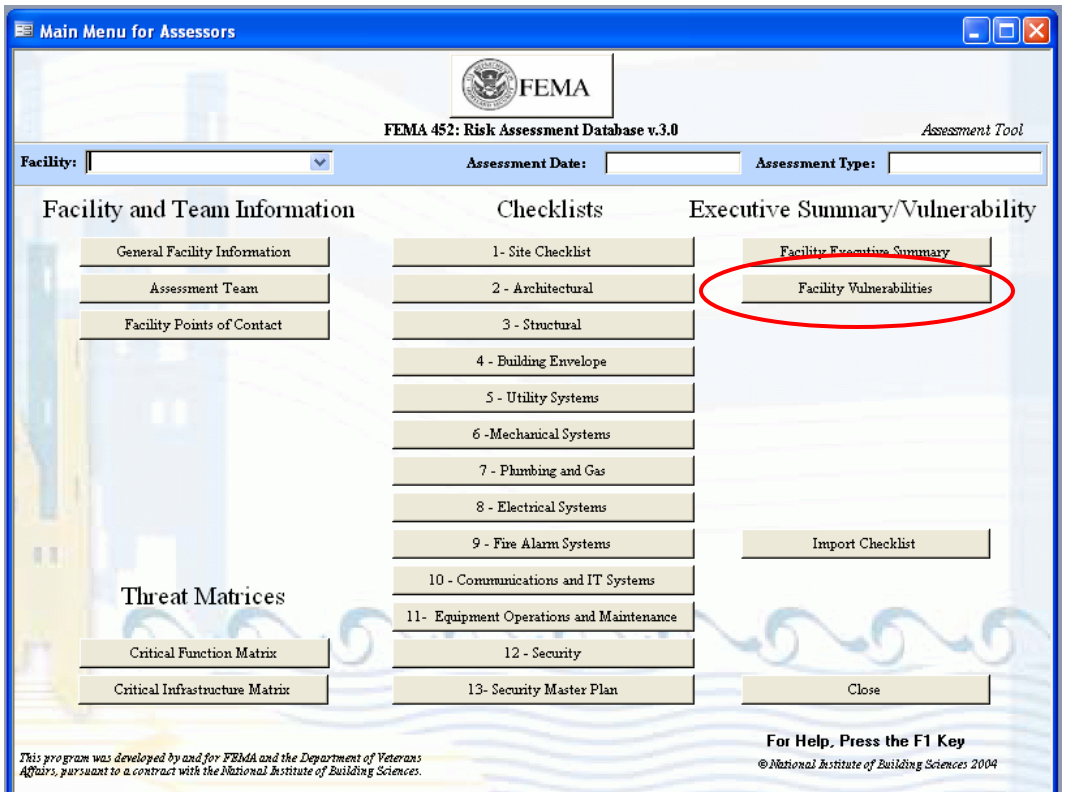
Note: The software indicates, using a pop-up, that more information – building number and priority – will be required when the Vulnerabilities screen is opened.

When all the information is input to the visible screen, you can scroll the screen using the right side vertical slide bar or use the Record selector arrows in the lower left corner to get to the question desired. Also, double clicking on the top blue bar will expand the window size to show a full screen of information.

The other Checklist sections all function the same way to capture observations and recommendations or remediation. As before, when finished, left click on the <Close> button in the lower right corner to go back to the Main Menu for Assessors screen.

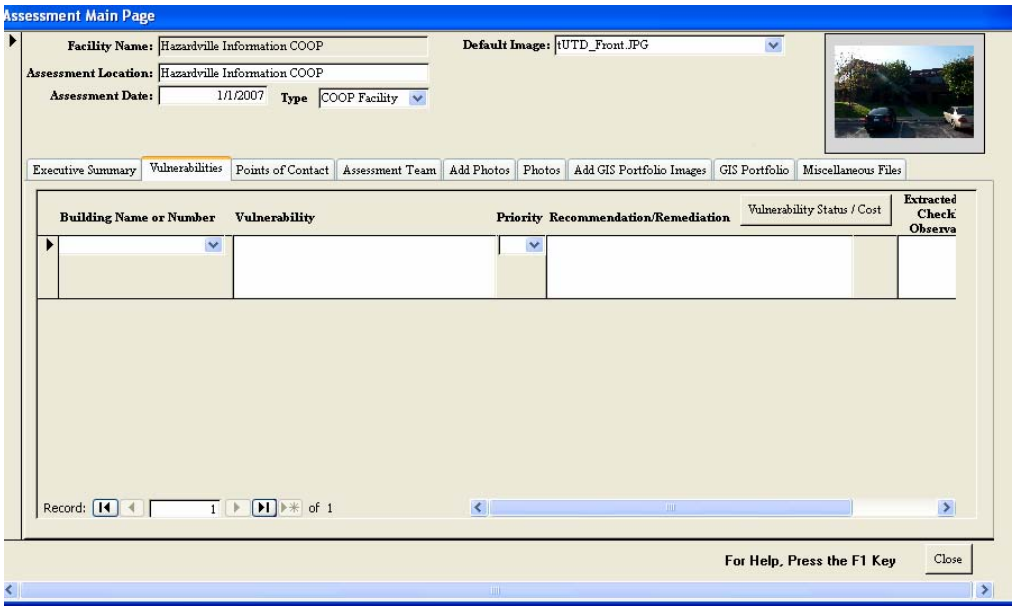
Facility Vulnerability Process

The Facility Vulnerabilities section of the Assessment Tool provides a means to further analyze the vulnerabilities found during the assessment. By displaying on one list the facility's vulnerabilities, their location and the initial recommended remediation, assessors can determine common weaknesses and mediation strategies that will work for multiple vulnerabilities. This also aids in the analysis of prioritization for mediation. Left clicking on the <Facility Vulnerabilities> tab will take you to that screen.



Vulnerability and Recommendation Screen

This is the Vulnerability and Recommendation screen of the Assessment Tool. It is automatically populated with the previously entered Observations (called Vulnerability here) and Recommendation / Remediation when the "Vuln?" box is checked when completing a question on the checklists. Note that the rightmost column of the page shows the checklist section from where vulnerabilities were transferred. Assessors can also populate the list by typing vulnerabilities onto the page (some may not be associated with a checklist question).



This screen has two fields that are still blank if a vulnerability was transferred from a checklist by clicking the "Vuln?" box.

- Record a building name or number in the first column to focus where this vulnerability is located.

- Prioritize the vulnerability so as to better identify which vulnerabilities require mitigation based upon the limited resources available – get the best benefit / cost ratio for reducing overall risk.

There are two other ways to get Vulnerabilities and Recommendations / Remediations into the fields:

- The assessors can type them directly into the fields. They will not show linkage to specific checklist questions unless that information is also added.

- Vulnerabilities and Recommendations / Remediations can be imported from the Assessment Tools of other assessors using the tool's import utility. In doing this,

the Lead Assessor has the option of importing all of a Team Member's vulnerabilities and recommendations, or choosing specific ones to transfer.

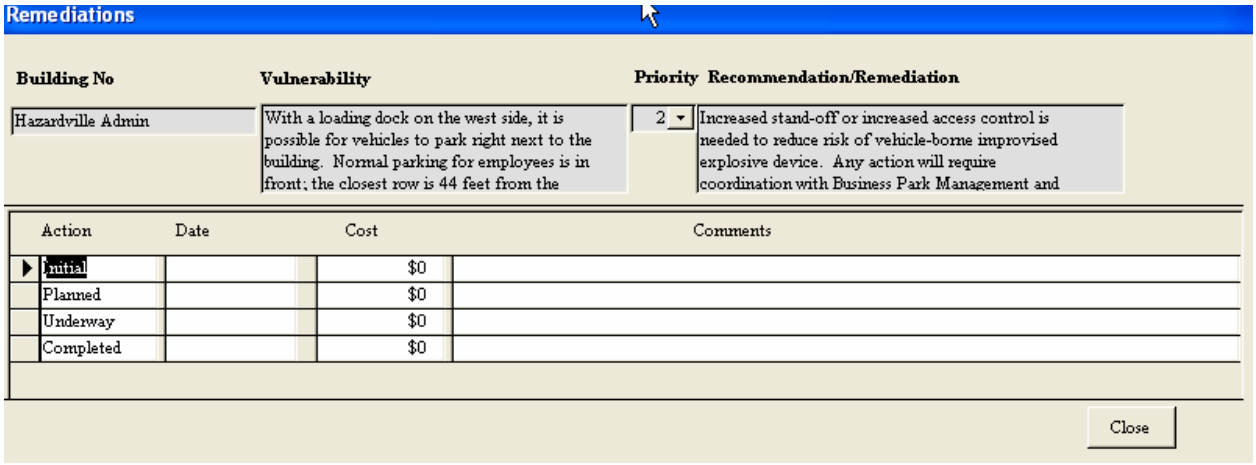
When an assessor identifies a vulnerability, the assessor must enter a building number and a priority number (1 to 5) in the Vulnerability List in addition to making recommendations about how to reduce the vulnerability/risk.

CAUTION: If you do not select a priority number before the inputs are accepted by the database, the number will be set to zero and this entry will come out on the top of the vulnerability report.

Prioritization is based on the severity of the vulnerability and the availability of resources for mitigation. For example: Priority 1 vulnerabilities are the most important to mitigate…fix it now. Priority 5 vulnerabilities may wait until additional funds are available.

The Master Database can be searched based on this field…all Priority 1 vulnerabilities, all Priority 1 and 2 vulnerabilities, etc.

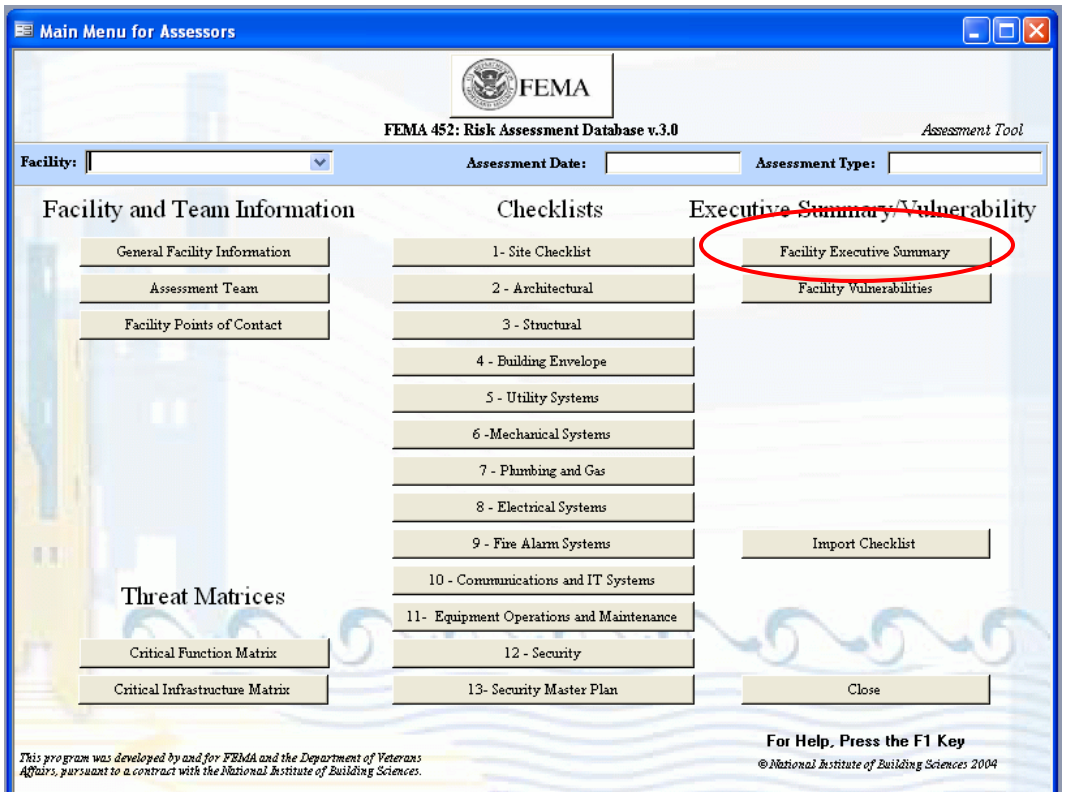
Finally, the Assessment Tool allows an assessment team to provide a cost estimate (dollar values) to the individual recommendations: New fence $100,000, Vehicle barriers $25,000, etc. Left click on <Vulnerability Status / Cost> from the Facility Vulnerabilities page to enter the Remediation module.



The Program Manager can then track the cost information throughout the process to implement the recommendation. Left click <Close> to exit the Remediations screen and left click <Close> to exit the Facility Vulnerabilities screen.

Facility Executive Summary Process

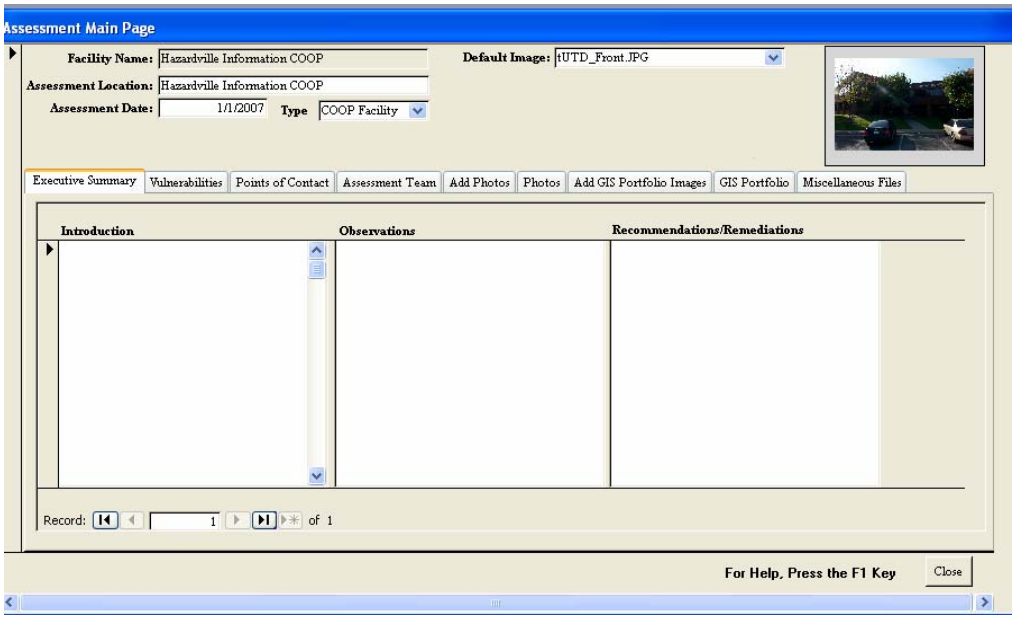
The Facility Executive Summary section of the Assessment Tool allows an assessor, usually the Team Leader, a page to summarize general information about the facility and this assessment. Left clicking on the <Facility Executive Summary> tab will take you to that screen.



Facility Executive Summary Menu

The Facility Executive Summary section of the Assessment Tool provides three fields for the Lead Assessor (or Team Leader) to summarize general information about the facility and this assessment. When printed, these three fields appear as a single document with three main sections: Introduction, Observations, Recommendations / Remediations.

The Introduction field should contain some background information, facility location, mission, dates, etc. The Observations field should contain general information about what was found, but particularly, vulnerabilities…are they security related, critical infrastructure related, etc. Finally, the Recommendations / Remediations field is for general recommendations about current conditions, mitigation measures that are applicable to the major vulnerabilities and other pertinent information to consider.



Note that you can use the tabs above the three fields to go from this section to many others to review information as necessary while writing the Executive Summary.

One word of caution regarding the Executive Summary: The import/export utility will not transfer this section of the tool between assessors, so if an assessment team member other than the Lead Assessor fills in these fields, there are two ways to transfer the information between laptops: one method is for the drafter of the Executive Summary to switch to Master Database mode, go to Facility Reports / Executive Summary / Publish as a Word Document / Save the Word Document where it can then be transferred to the Lead Assessor as a Word Document file. An alternative is to cut and paste the three paragraphs into a document and transfer the temporary document between computers. Then the Lead Assessor can cut and paste the individual paragraphs back into the Executive Summary.

Use <Close> to return to the Main Menu for Assessors Screen.

Importing Checklists, Vulnerabilities and Recommendations

After the assessment team has completed its data collection effort, the checklist questions, vulnerabilities, and remediations have to be combined into one Assessment Tool database before the data can be transferred to the Master Database. This is accomplished by using the import function to transfer collected data from the Team Members Assessment Tool Databases to the Lead Assessor's Assessment Tool Database.

Let's say there are five members of the assessment team: A Lead Assessor, a Security Specialist, a Mechanical/Electrical Assessor, a Structural Engineer, and a Cost Estimator. Before the start of the assessment, the Lead Assessor (or Team Leader) should assign Checklist sections to each member of the team. For example, the Structural Engineer would do Checklist Sections 2, 3 and 4. Checklist sections can be split among team members; this makes importing more complex, but still doable.

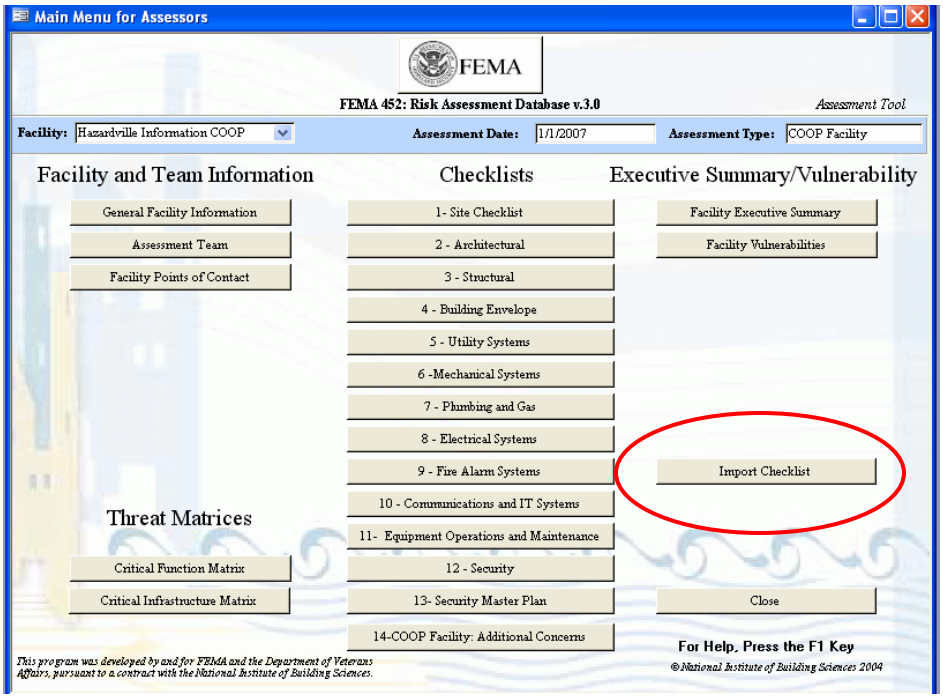
The import utility of the Assessment Tool allows the Lead Assessor to collect checklist observations and comments, along with vulnerabilities and the associated recommendations from the team members. This consolidated database is the responsibility of the Lead Assessor to ensure technical editing, consistency, and a flowing report to become part of the Master Database.

The process is simple but it takes some practice.

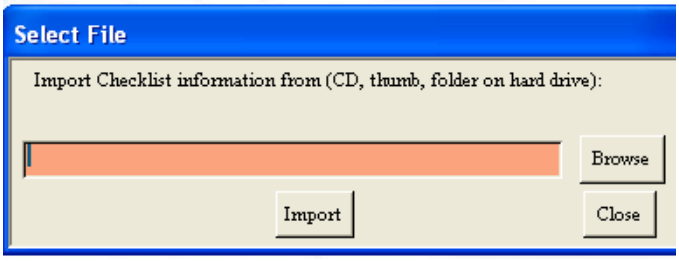
- Each team member must copy his Assessment Tool database file to a transfer device. A USB drive works well as a file transfer device. The file will be a large (several dozen MB) Microsoft Access© MDE Database file.

- The Lead Assessor inserts the USB drive into his own laptop and copies the file into the same folder of his database. Then, from the Main Menus for Assessors, the Lead Assessor should select the facility being assessed from the pull down list, and click on the <Import Checklist> button.

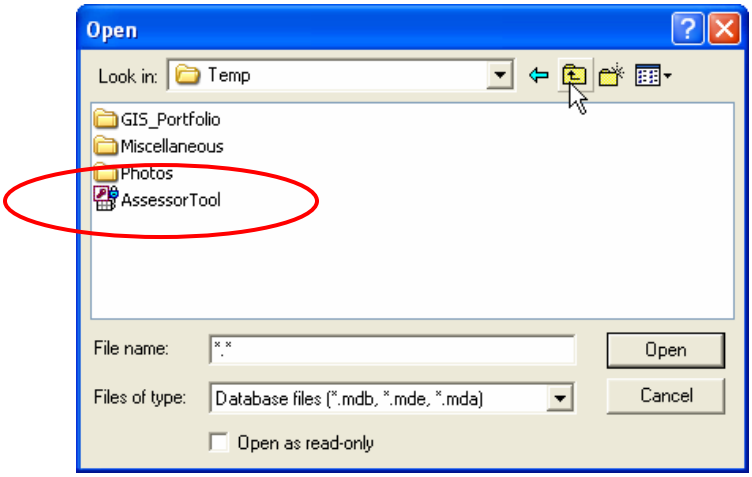
Note: First, ask your database administrator to make sure the Lead Assessor user name is assigned to the "Admins" group. If you are not in the "Admins" group, the Import Checklist button will be grayed out and not functional.



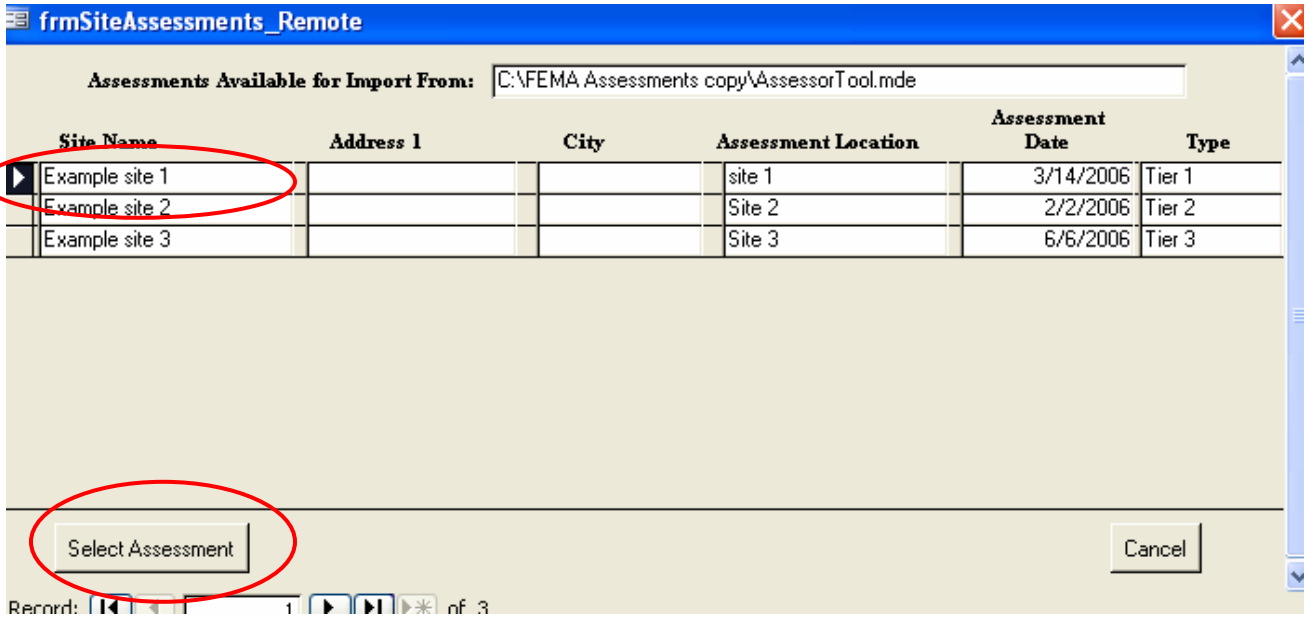
This brings up a request window to identify the file to select for import. Left click <Browse> to find the file.



After finding the database file either double left click on the file or left click once on the file and then left click the <Open> button to have the file name and location appear in the field. Finish the process by left clicking on the <Import> button.



This will bring up a window listing all the available assessment facilities available to import from. Click on the assessment facility you want to connect to, then click <Select Assessment> to establish a connection between databases.

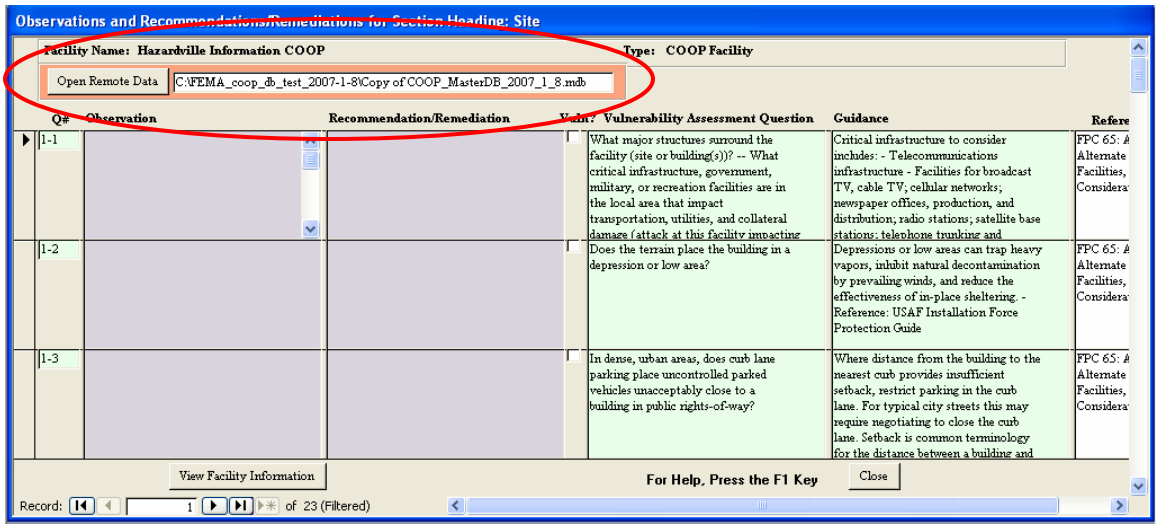


This will bring up a small window to indicate the connection between databases has been made, and # Checklist records and # Vulnerability records are available for viewing and copying to the Lead Assessor's database.

Warning: It is important to realize that the wrong database can be imported as easily as the correct one. It is imperative for the Lead Assessor to keep accurate track of files copied from other assessors.

Viewing and Importing From Linked Databases

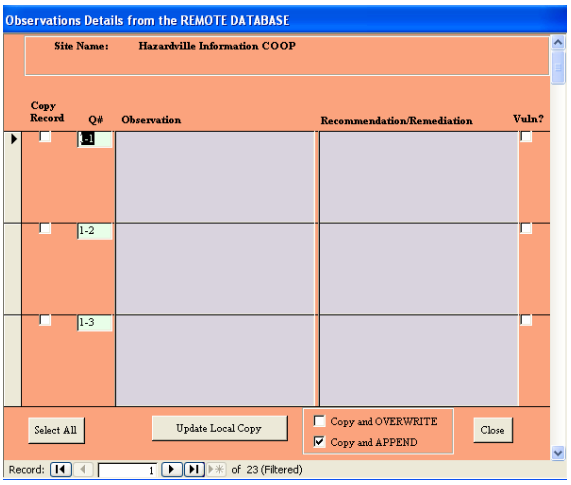
The next step is for the Lead Assessor to select the Checklist section that he wants to import data into. Then left click <Open Remote Data> to open the orange import window.



The “remote data” is the database to be imported, identified with orange backgrounds.

Section 1, Site Checklist, is shown here in the screen capture. The Lead Assessor can then select the specific observations and comments to be imported by putting a check mark in <Copy Record> or choose <Select All> to input all Observations and Recommendations / Remediations in this section. The Lead Assessor can also decide to add the new information to any he already has entered by indicating by check mark to <Copy and Append> or overwrite anything previously entered using <Copy and Overwrite>. The default is Copy and Append.

Warning: Make sure you track what you are importing. This is where it is possible to accidentally overwrite good data with a blank field.



The process is the same for importing vulnerabilities and recommendations.

This is a very handy tool, allowing the Lead Assessor to assemble all of the collected data on one database and in one computer before leaving the facility at the end of the assessment.

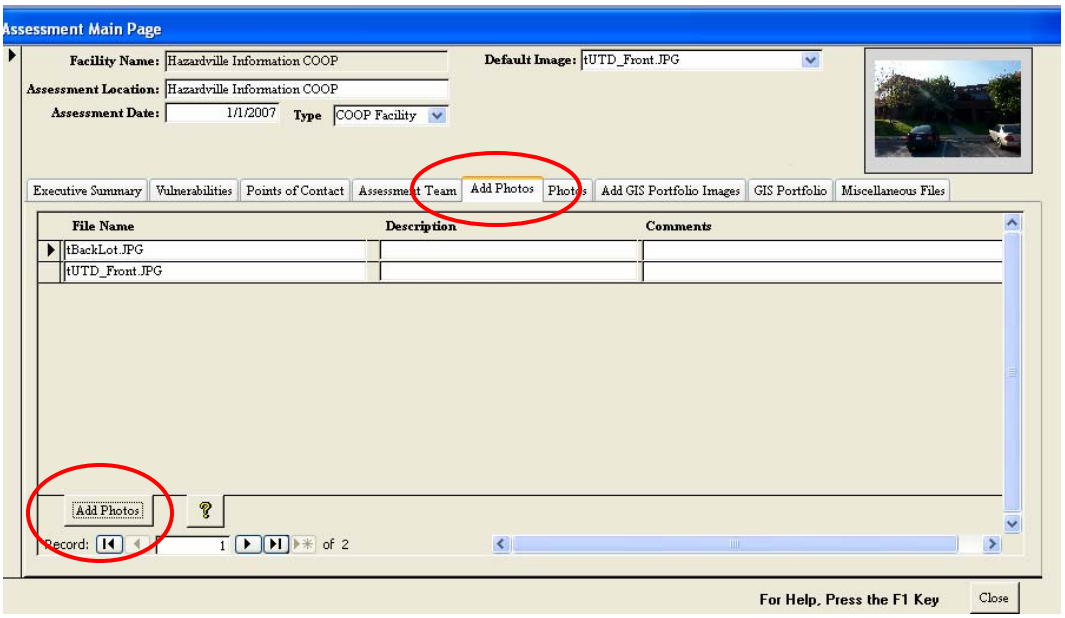
Note, however, just as the GIS Portfolio Images, Miscellaneous Files, and Photos had to be placed into the appropriate subfolders in the Assessment Tool program folder, each team member must also provide these files on the USB drive for transfer to the Lead Assessor's computer.

Adding Photos

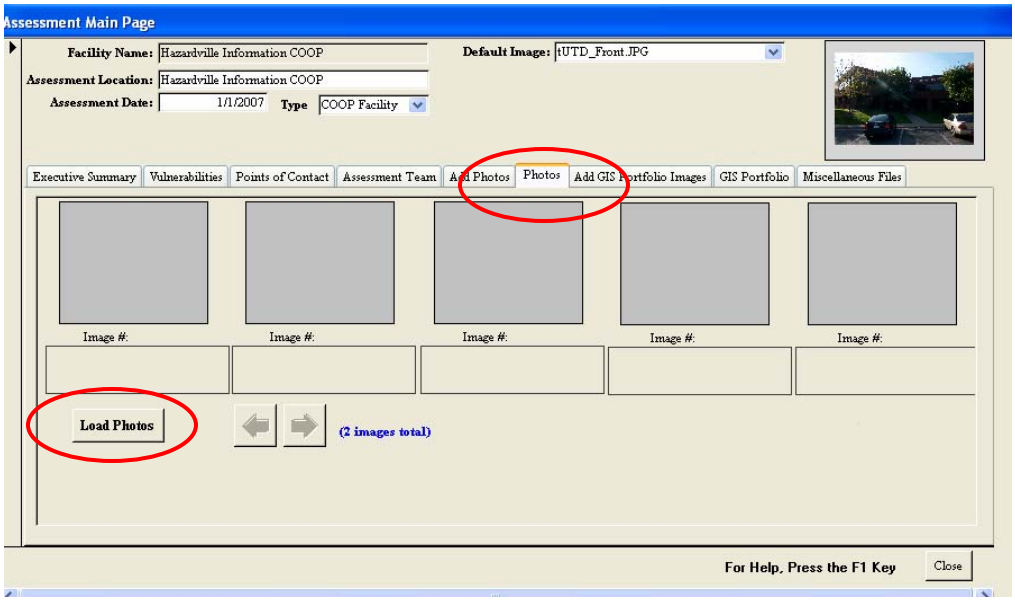
Even though you have placed the GIS Portfolio, Miscellaneous Files, and Photos into the proper subfolders, you must still link them to the database. To do this for photos taken by the assessment team:

- Go to the Assessment Tool Main Menu. Select <Assessments>, select <Facility Vulnerabilities>, and select <Add Photos>.

- In the Add Photos screen left click the <Add Photos> button in the lower left corner.



- The software confirms that the files were added and attached. Left click <OK> to continue with each pop up.



- Next you have to left click on the <Photos> tab in the center of the screen to continue the process.

- Once in the Photos screen, left click on the <Load Photos> button in the lower left corner, which makes the linked photos visible within the Assessment Tool. You can left click on a photo and enter Photo Zoom which gives a limited capability for viewing the photo in different sizes, using Zoom, Clip, and Internet Explorer. Clip is essentially what you currently see. When done, left click <Close> to exit.

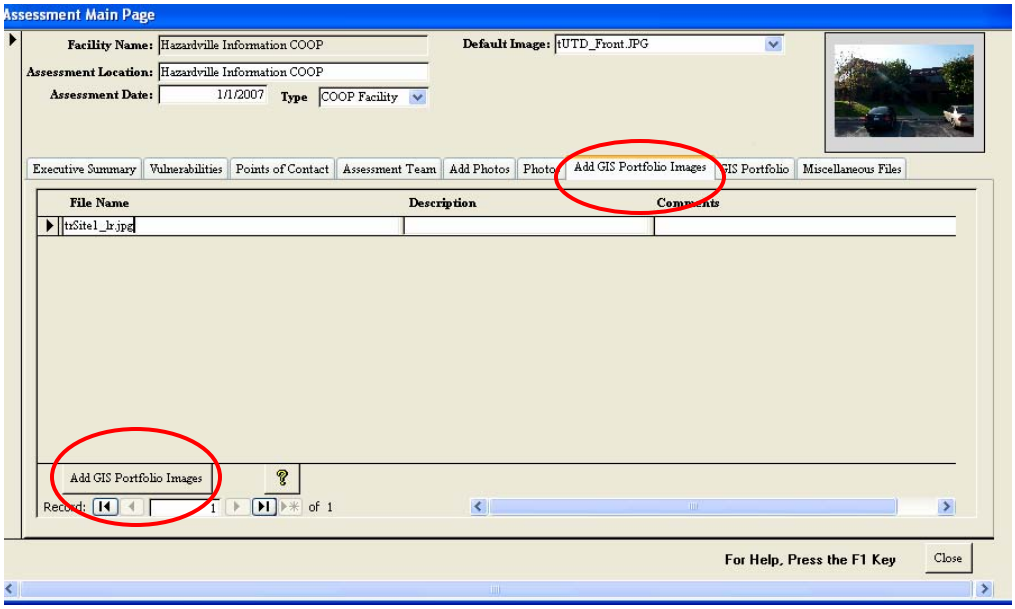
Adding GIS Images

Even though you have placed the GIS Portfolio, Miscellaneous Files, and Photos into the proper subfolders, you must still link them to the database. To do this for GIS images:

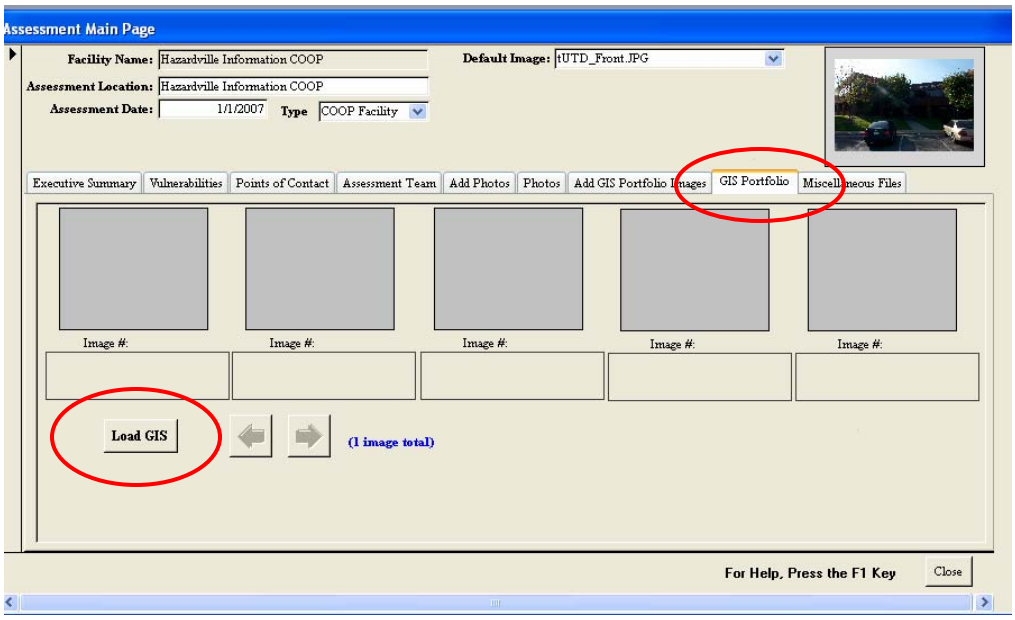
- Go to the Assessment Tool Main Menu: Select <Assessments>, select <Facility Vulnerabilities>, and select <Add GIS Portfolio Images>.

- In the Add GIS Portfolio Images screen first left click the <Add GIS Portfolio Images> button in the lower left corner.

.



- The software confirms that the files were added and attached. Left click <OK> to continue with each pop up.



- Next you have to left click on the <GIS Portfolio> tab in the center of the Assessment Main Page screen to continue the process.

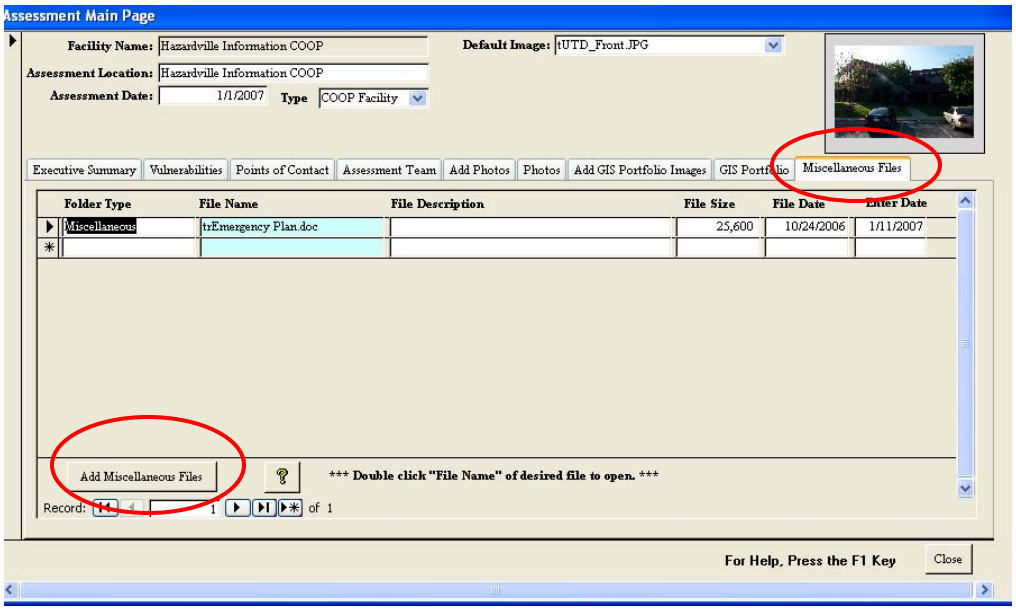
- Once in the GIS Portfolio screen, left click on the < Load GIS > button in the lower left corner, which makes the linked photos visible within the Assessment Tool. You can left click on a photo and enter Photo Zoom which gives a limited capability for viewing the photo in different sizes, using Zoom, Clip, and Internet Explorer. Clip is essentially what you currently see. When done, left click <Close> to exit.

Adding Miscellaneous Files

Even though you have placed the GIS Portfolio, Miscellaneous Files, and Photos into the proper subfolders, you must still link them to the database. To do this for Miscellaneous Files:

- Go to the Assessment Tool Main Menu: Select <Assessments>, select <Facility Vulnerabilities>, and select <Miscellaneous Files>.

- In the Miscellaneous Files screen left click on the <Add Miscellaneous Files> button in the lower left corner.



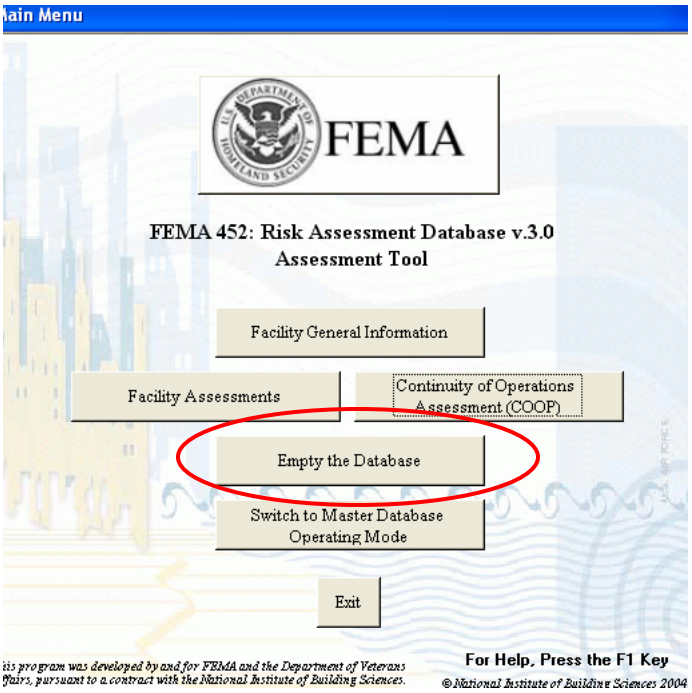
- The software confirms that the files were added and attached. Left click on <OK> to continue with each pop up.

Files can then be viewed by left clicking on the File Name.

Erasing All Assessments in the Database

Administrators have the capability to erase all records in a database, **permanently**. This is only done after transferring your data to a Master Database **on a separate computer** and when starting a new assessment. This enables an administrator to remove all database entries and start with an empty database. It also serves to control assessment information. Note: this is permanent. **Confirm you have transferred the information to the Master Database on a separate computer before you erase the data.**

Left click on <Empty the Database>. The next window confirms that you want to **permanently** erase all assessment data. Left click on <Yes> to continue or cancel.



Warning, confirm you have transferred the information to the Master Database **on a separate computer** before you erase the data.

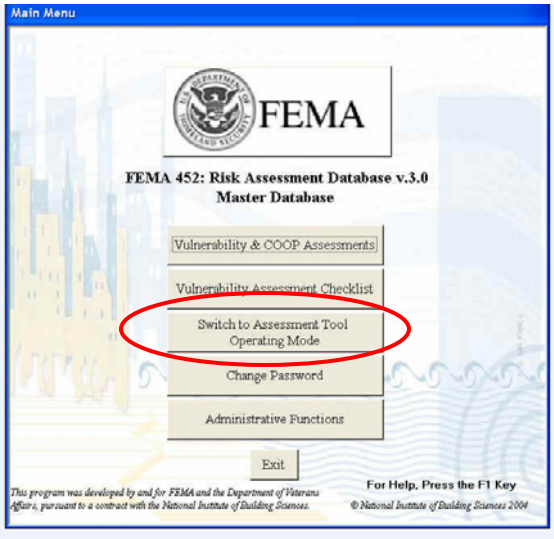
Switching Between Operating Modes

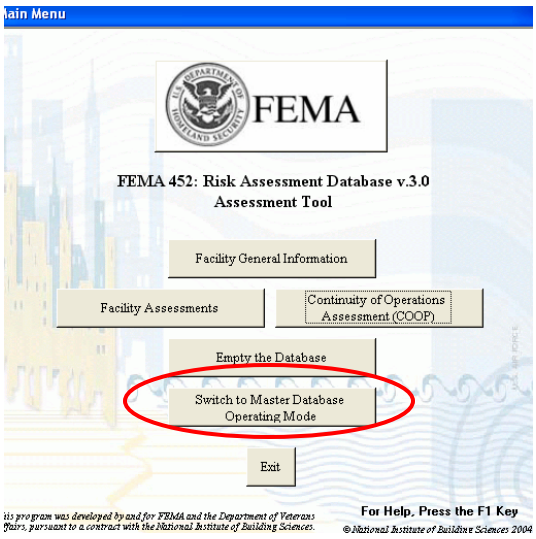
The <Switch Operating Modes> tab takes you between the two operating modes: Assessment Tool mode and Master Database mode.

An organization will generally use two different copies of the database: one loaded on a laptop and operating in the Assessment Tool mode for conducting assessments in the field, and the other loaded on a computer at your organization's headquarters and operating in the Master Database mode for collecting the results from the assessors, printing reports, and archiving the results from a number of assessments. The Master Database copy also provides the organization the ability to search for vulnerabilities common to many assessed facilities, search for specific vulnerabilities, etc. Essentially it can be used as a Risk Management tool to identify and track mitigation measures to reduce risk.

The Assessment Tool mode was designed for engineers and security specialists to be able to easily collect data from the facility being assessed. As you will see, the software is very user friendly. The Master Database mode was designed for the Program Manager.

Switching between the main page of the Assessment Tool to the Master Database mode is as simple as left clicking on the <Switch Operating Modes> button.





The next window confirms that you want to switch modes. Left click on <Yes> to continue or the other buttons if you do not want to change modes. Then another confirmation window pops up. Left click on <OK>.

Left click on <Exit> to close the Database.

Master Database Mode

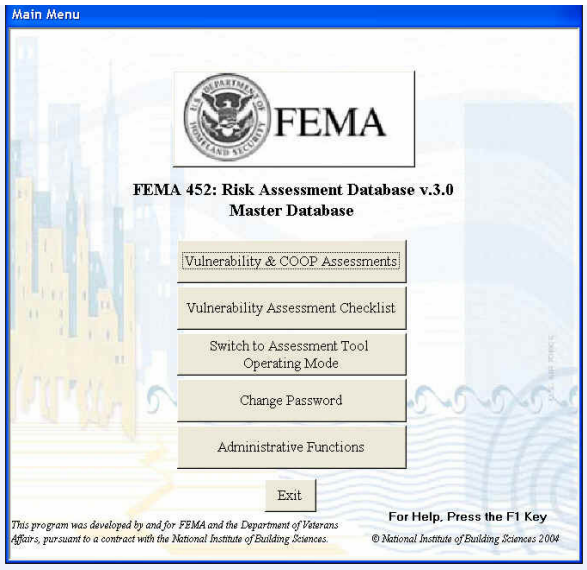
An organization will generally use two different copies of the database: one loaded on a laptop and operating in the Assessment Tool mode for conducting assessments in the field, and the other loaded on a computer at your organization's headquarters and operating in the Master Database mode for collecting the results from the assessors, printing reports, and archiving the results from a number of assessments. The Master Database copy also provides the organization the ability to search for vulnerabilities common to many assessed facilities, search for specific vulnerabilities, etc. Essentially it can be used as a Risk Management tool to identify and track mitigation measures to reduce risk.

The Assessment Tool mode was designed for engineers and security specialists to be able to easily collect data from the facility being assessed. As you will see, the software is very user friendly. The Master Database mode was designed for the Program Manager.

Master Database Main Menu

The initial screen of the Master Database mode leads to four functions:

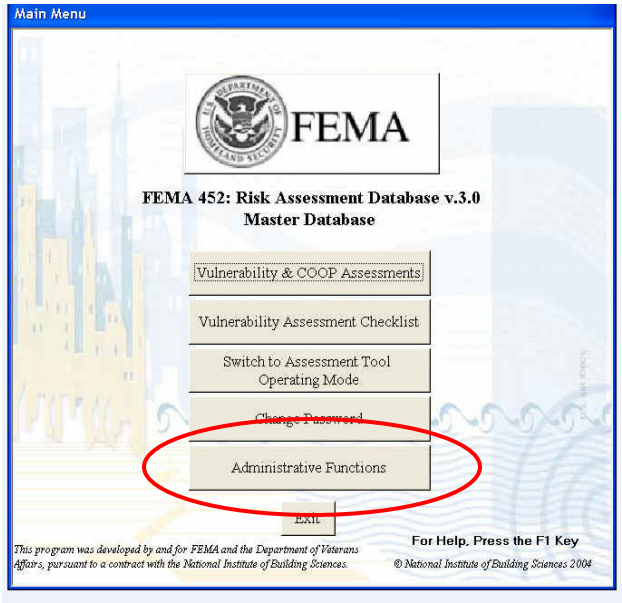
- Manage Assessments by clicking on the <Assessments> button.
- View the Vulnerability Assessment Checklist by clicking on the < Vulnerability Assessment Checklist > button.
- Switching to the Assessment Tool operating mode by clicking on the < Switch to the Assessment Tool Operating Mode> button.
- Change Passwords by clicking on the < Change Password> button.
- Perform Administrative Functions by clicking on the < Administrative Functions> button.



To use the Master Database, the first step is to import an assessment from the Lead Assessor's Assessment Tool. This is an Administrative Function and will be covered first, followed by the functions. Note: administrative functions are not available to all users. Only those logged with administrator permission can use the administrative functions. For example, only administrators may import assessment information from Assessment Team Leaders to the Master Database.

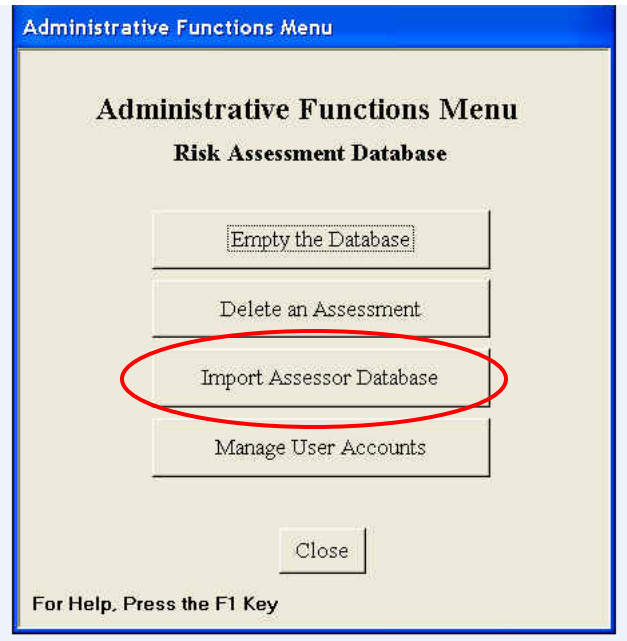
Administrative Functions

One of the most important feature needed to understand about the Master Database is – how to import the Lead Assessor's Assessment Tool database into the Master Database. To begin this process left click on <Administrative Functions> from the Main Menu.



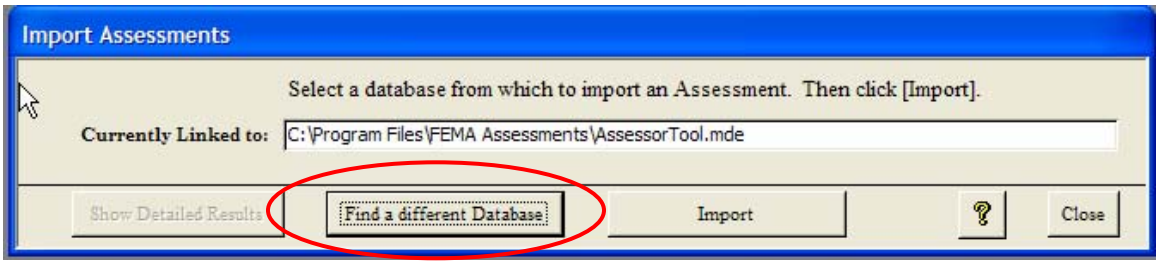
Importing Assessment Tool Databases

To proceed, left click on the <Import Assessor Database> button in the middle of the Administrative Functions Menu. The other buttons function the same as in the Assessment Tool, except that it applies to the Master Database.



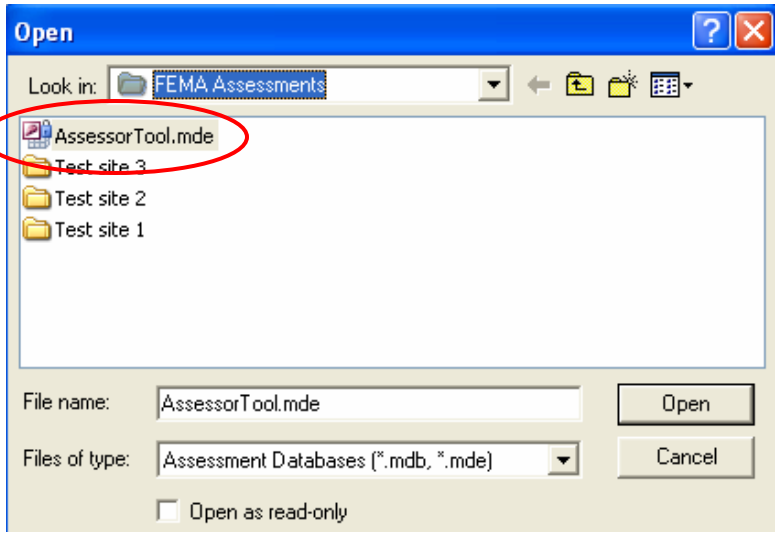
Note: If the <Import Assessor Database> button is grayed out, it means that you have entered the Master Database by switching modes from the Assessment Tool, having logged in as Assessor vice as Administrator. To Import, always enter the Master Database an Administrator.

The next step is to find the Assessment database to import. This screen opens with the file identified to which the Master Database is currently linked.

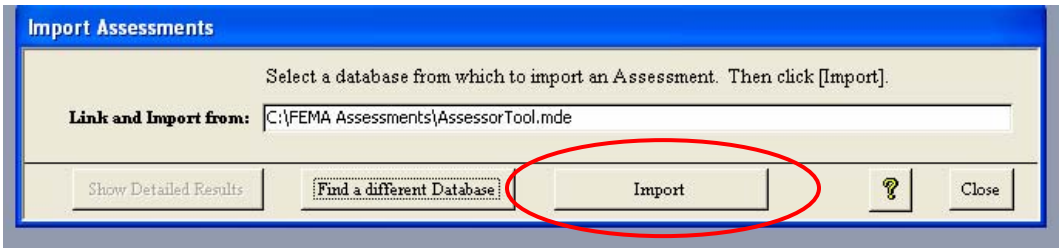


Left click on the <Find a different Database> button to find the Assessment database that you want to import.

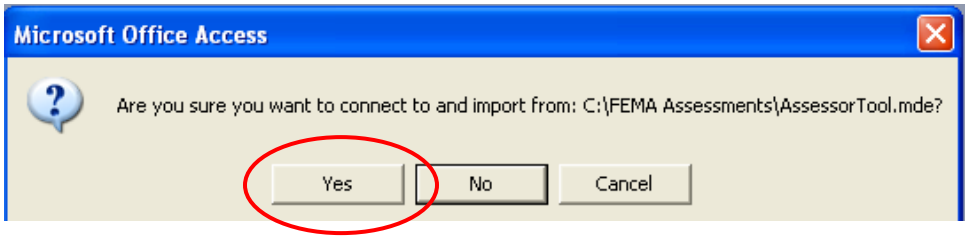
With this screen you identify the Assessment database that you want to import into the Master Database. Single left click on the file to import, which will put that file into the File Name window which then requires a left click on the <Open> button OR double left click on the file to link to this file.



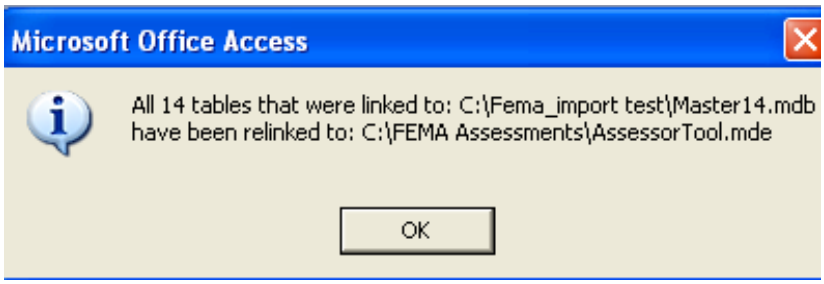
Returning to the Imports Assessments screen the Link and Import window now correctly identifies the database to be imported. Now left click the <Import> button to initiate the import.



A confirmation screen then pops up to ensure this is the desired action for the indicated file. Left click on <Yes> to continue.



The import function confirms the linking to the desired database has been accomplished. Left click on <OK> to continue.

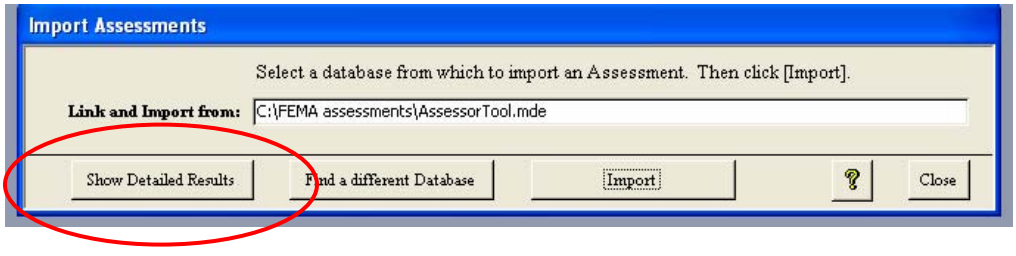


A screen opens with a list of facilities that can be imported. Place the arrow on the facility to be imported and left click on < Select Assessment>.

Instead of manually moving the files in these subfolders between locations as in the Assessment Tool, the import function of the Master Database allows a one-button operation to do the same thing. Left click on <Yes> to make these transfers. Note: the files must be in the same folder as the database being imported. Also, if there are no files in a given folder, the computer will let you know.

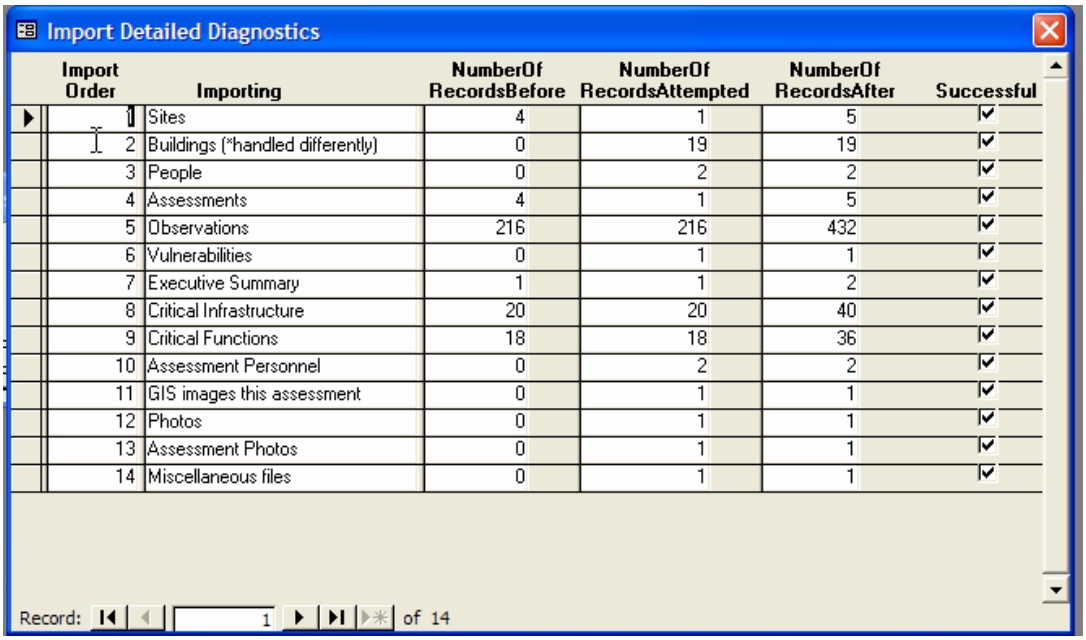
The final confirmation pop-up you will see will ask if you want to write the files now. Left click <Yes> to complete the import process.

As in every process, it is always necessary to confirm that what you wanted to have done was actually done. Left click on <Show Detailed Results> to check that all transfers were successful.



The Import Detailed Diagnostics screen shows what was in the Master Database before the import, the number of records attempted by the import, and the records after the import. The quick check is to scan the right hand Successful column to ensure all boxes are checked.

Another check is to scan Row 4, Assessments. The number of assessments in the Lead Assessor's database being imported should match the number of assessments attempted. This is also one of the few times you left click on the X box in the upper right corner to close the window and return to the previous screen.

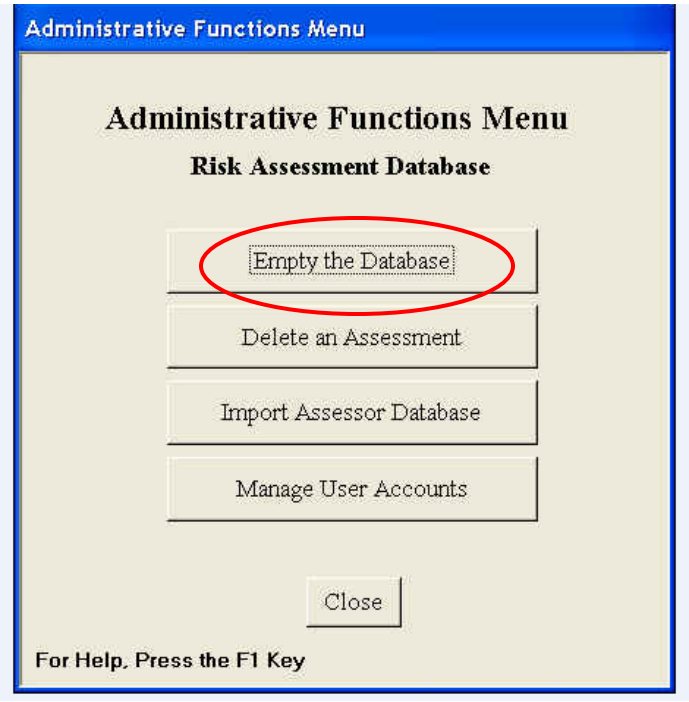


That completes the import function.

Erasing All Assessments in the Database

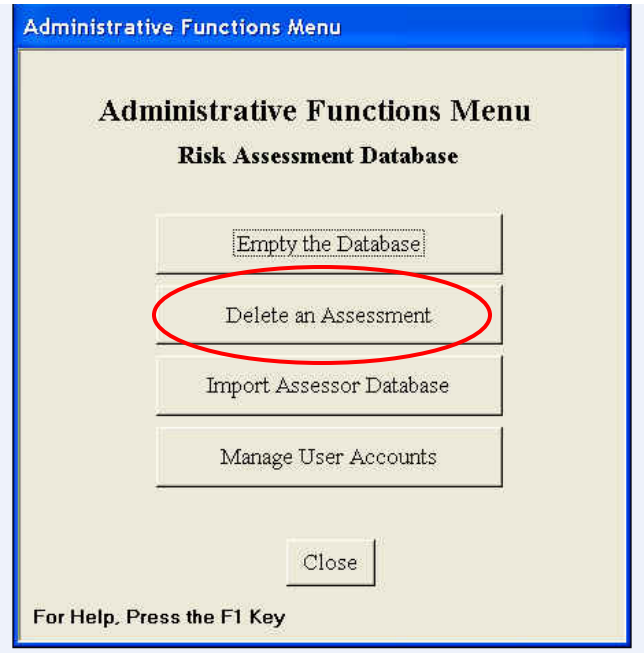
Administrators have the ability to erase all records in the database, **permanently**. This is usually only done when starting a new program on a new computer. Selecting the <Empty the Database> button opens a confirmation window, to ensure you want to permanently erase all assessment data. Left click on <Yes> to continue or cancel.

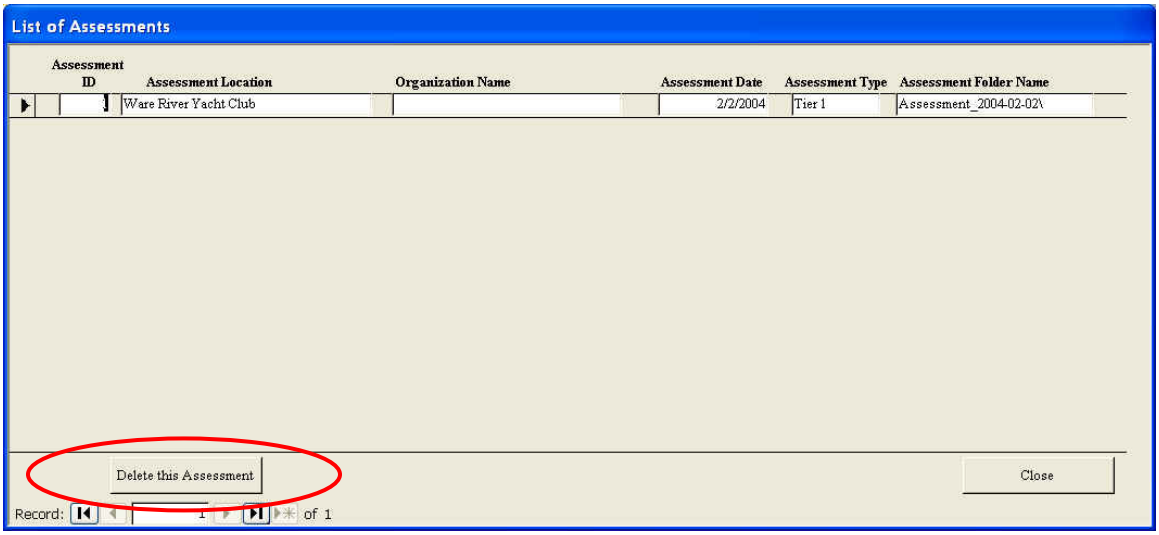
Warning: this will erase all records in the database, **permanently**!



Erasing a Single Assessment in the Master Database

Administrators have the ability to erase a single assessment in the database, **permanently**. This is usually only done when an assessment was loaded in error. Selecting the <Delete an Assessment> button opens a list of assessments. Select the assessment to erase, then left click <Delete This Assessment>. This will open a confirmation window, to ensure you want to permanently erase the selected assessment. Left click on <Yes> to continue or cancel.





Warning: this will erase the assessment from the database, **permanently**!

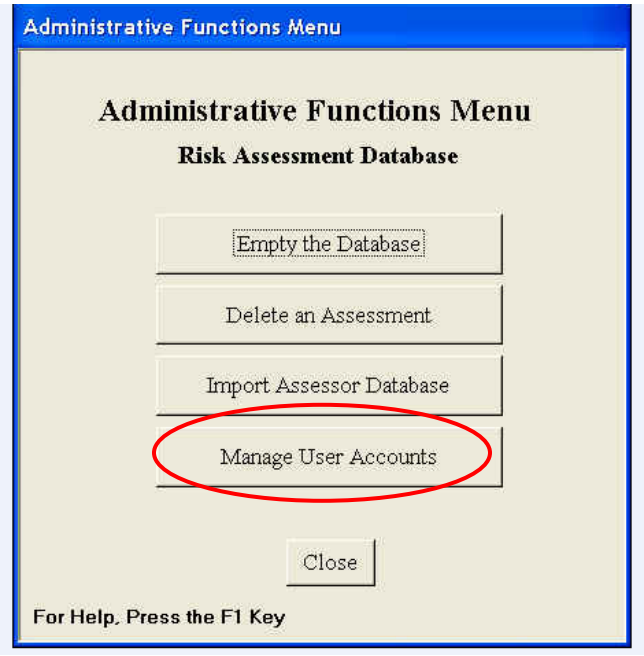
Manage User Accounts

The <Mange User Accounts> button enables an administrator to add a new user, delete a user and assign permission levels to users. The database is preloaded with the following four users:

Name: Administrator	**Password**: Administrator
Name: Assessor	**Password**: Assessor
Name: Editor	**Password**: Editor
Name: Reader	**Password**: Reader

These are examples only and should be changed after installing the program. Note that the password and for the four original users can change, but these four users can not be deleted.

Select <Mange User Accounts> to start the process.



Add New User, Delete User, and Change Groups

After selecting Select <Mange User Accounts>, the form labeled “List of Users and the Group to which they belong” is displayed. From this form, an Administrator can add a new user, delete a user and assign or change their permission level, called Group.

User Groups:

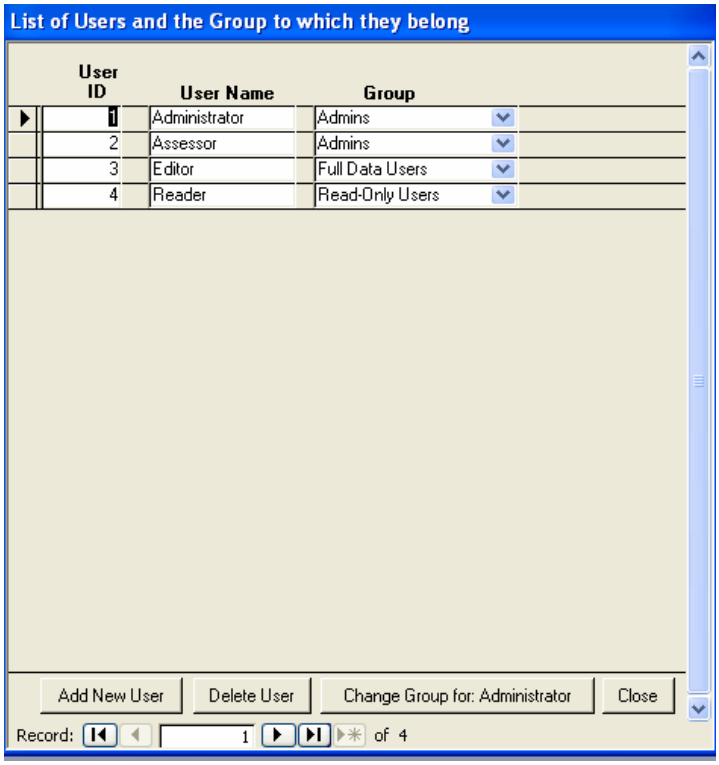
Three user groups have been created for the database in the Workgroup File: *Admins*, *Full Data Users*, and *Read Only Users*.

Admins has full access to the database. The Administrative Functions button will only be visible for users in the Administrator group. One user has been created in this group, Administrator. It has the initial password of "Administrator". It is highly recommended to assign "Administrator" a different password in the Master Database after initial logon.

Full Data Users can view and update data. The created users "Assessor" and "Editor" have the an initial passwords of "Assessor" and "Editor" respectively.

Reader can only view data. The created user "Reader" has an initial password of "Reader".

These are examples only and should be changed after installing the program. Note that the password and permission level for the four original users can be changed, but these four original user accounts can not be deleted.



Add a New User:

From the form labeled "List of Users and the Group to which they belong", select <Add New User> button to add a new user name to the database. A screen opens called "Add a new USER Account". On this screen, type in the new user name and select from the drop down box users group (permission level). After making entries, left click on the <Add User> button to finalize the account.

Delete a User:

The first step is to select one of the existing Users by left clicking on the far left column of the form labeled “List of Users and the Group to which they belong”. This will mark the User desired with a right pointing arrow head if one is not already there. This selects the User and links the buttons across the bottom to that User.

Next left click on the <Delete User> button to delete a user name from the database. A warning screen opens asking you to confirm the deletion. Left click <YES> to continue, or <NO> or Cancel> cancel the action.

Change a User’s Group:

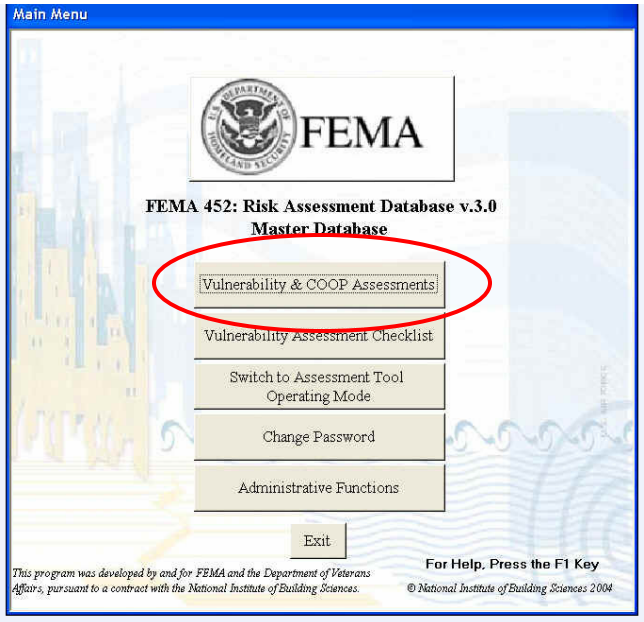
The first step is to select one of the existing Users by left clicking on the far left column of the form labeled “List of Users and the Group to which they belong”. This will mark the User desired with a right pointing arrow head if one is not already there. This selects the User and links the buttons across the bottom to that User.

Nest left click on the <Change Group for:…> button to change the group of a user from the database. Notice that name of the User selected on the top of the form is displayed in the button <Change Group for:…>. This is designed to help the Administrator keep track

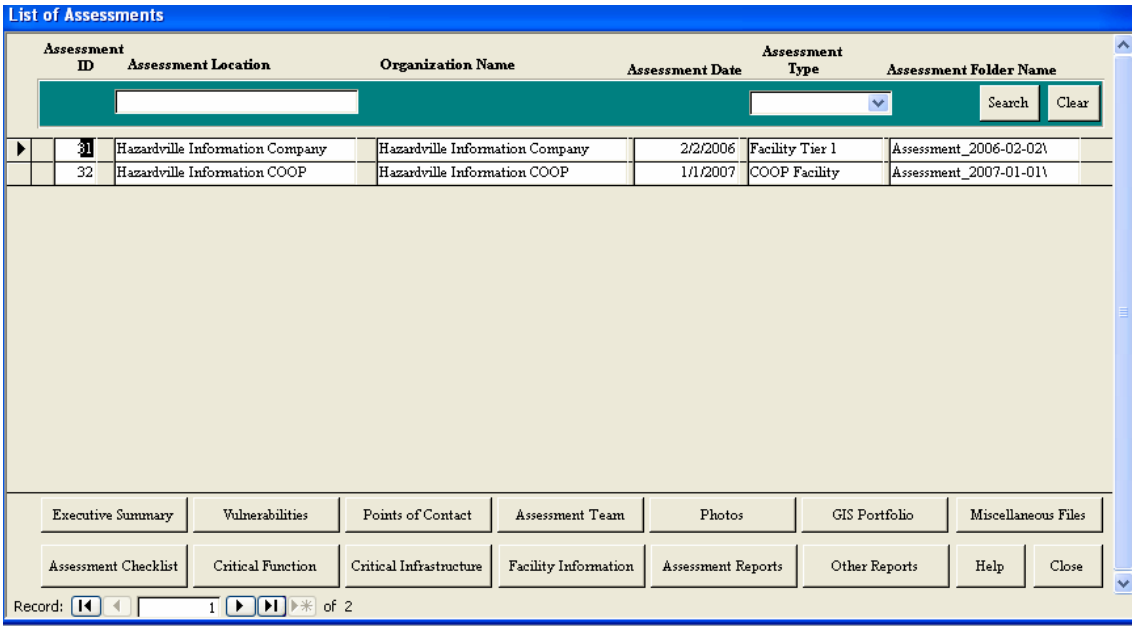
of the account they are working on. A screen opens asking you to select a Group from a drop down Menu. Left click <Change Group> to continue or Cancel> cancel the action.

Master Database Vulnerability and COOP Assessments Function

The Vulnerability and Coop Assessment Function gives the Project Manager or an assessor the ability to review assessment data, photos and files, search for specific observations, vulnerabilities, etc., and print reports from individual facilities or from the results of the searches. To begin this process left click on the < Vulnerability & Coop Assessments > button from the Main Menu.



This form provides the Project Manager the ability to review assessment data, Photos and files, search for specific observations, vulnerabilities, etc., and print reports from individual facilities or from the results of the searches.

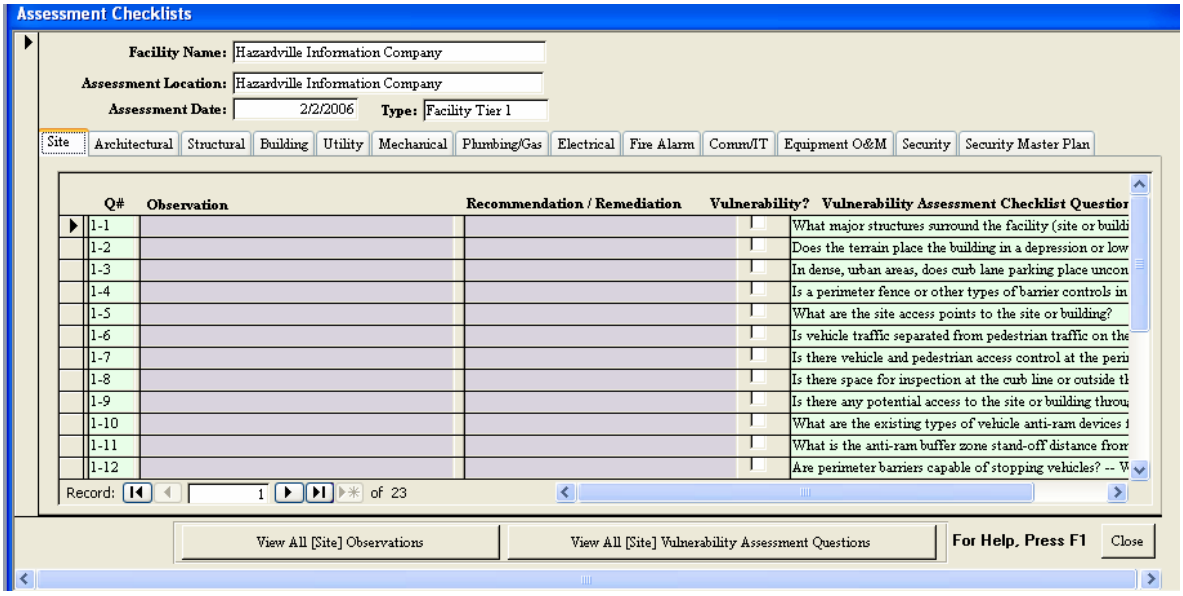


- The first step is to select one of the assessments by left clicking on the far left column of the List of Assessments. This will mark the assessment desired with a right pointing arrow head if one is not already there. This selects the assessment and links the buttons across the bottom to that assessment.

- Most Master Database screens mirror those in the Assessment Tool operating mode. The Assessment Checklist, Facility Reports, and Other Reports functions are unique to the Master Database operating mode. These new sections will be covered next.

Assessment Checklists

As can be seen, the initial screen is a summary type slide showing the Site Checklist questions.



- Only the first line of each Observation and Recommendation / Remediation is visible from this view, along with the “Vulnerability?” checkbox.

- Double clicking on any cell of a row retrieves screens that look much the same as in the Assessment Tool. Selecting green cells shows the entire question and any guidance. Selecting a purple cell displays a specific question and the data entered.

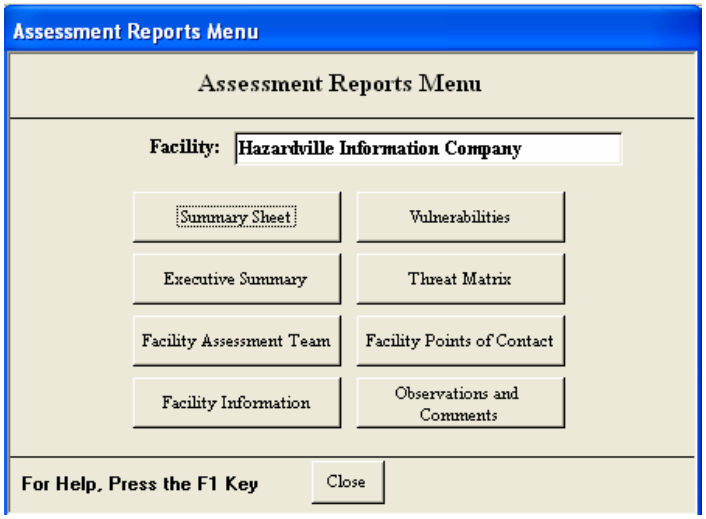
- Alternately, left clicking on the <View All [Site] Observations> button will expand the Checklist questions and show what has been entered in Observations and Recommendations. This also looks much like the Assessment Tool data entry screen.

- Similarly, left clicking on the <View All [Site] Vulnerability Assessment Questions> will make the Questions and Guidance more accessible and easier to read.

- This module can be used by the Administrator / Manager to edit inputs from the field. Anything typed into the purple fields becomes part of the record for the facility. However, clicking the “Vulnerability?” block will not automatically copy information to the Vulnerability list. This can only be done by entering the checklist from the Assessment Tool.

- Left click on <Close> to return to the List of Assessments.

Assessment Reports Menu



First choose an assessment facility indicated by the arrow in the first column of the List of Assessments page.

This menu is displayed when selecting the <Assessment Reports> button from the List of Assessments screen. From this location the user can print any of the automated reports for the assessment facility specified at the top of the menu (the selected record on List of Assessments for when the <Assessment Reports> button was depressed). Each report can be printed or converted into Microsoft Word© for editing, distribution, etc. Pressing the <Close Report> button returns to the Reports Menu.

- The <Summary Sheet> button produces the Facility Summary Sheet report.
- The <Executive Summary> button produces the Executive Summary report.
- The <Facility Assessment Team> button produces the report listing the information for the individual assessors responsible for that particular assessment.
- The <Facility Information> button produces the report listing the information for the individual assessment facilities.
- The <Vulnerabilities> button produces the Vulnerabilities and Recommendations/Remeditations report.
- The <Threat Matrix> button will perform an automated process which opens a Microsoft Excel© document and then populates it with the information for both the Critical Function Matrix and the Critical Infrastructure Matrix.

- The <Facility Points of Contact> button produces the Facility Points of Contact report.

- The <Observations and Comments> button creates the Assessment Observations and Comments report.

Click on the <Close> button at the bottom of the Assessment Reports Menu to return to the List of Assessments page.

Other Reports Menu

This menu appears after the user selects the <Other Reports> button at the bottom of the List of Assessments form. This area of the Master Database allows the Administrator / Manager to search for data from all assessments on file in the database. This is a very powerful analytical tool.

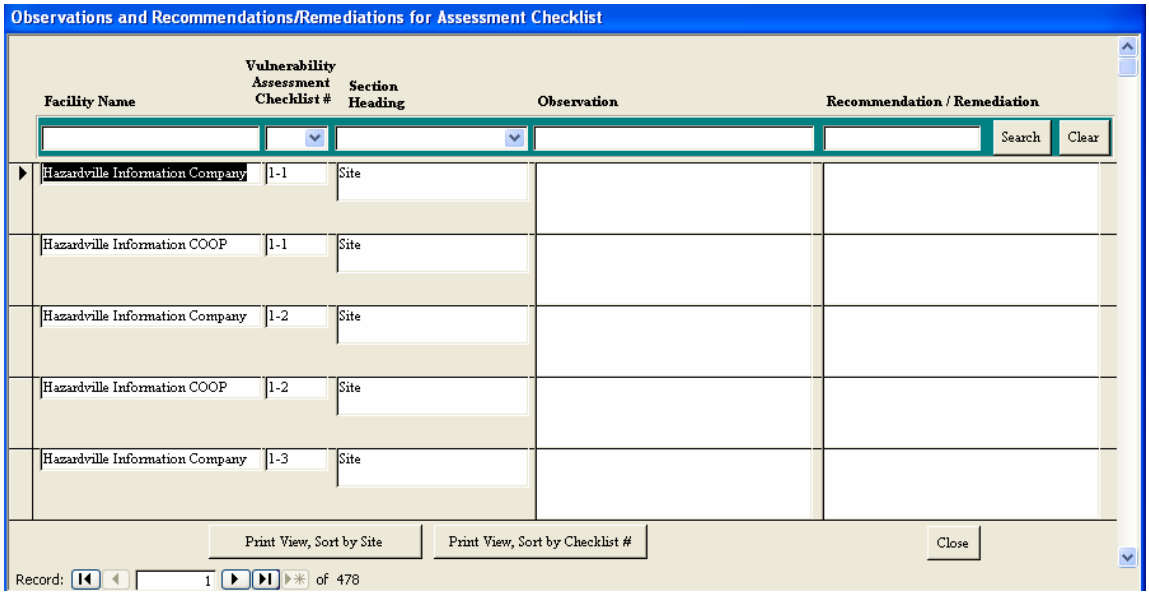
- The <Search Observations and Recommendations / Remedations> button opens the Observations and Recommendations / Remediations for Assessment Checklist form.

- The <Search Vulnerabilities and Recommendations / Remediations> button opens the Vulnerabilities and Recommendations/Remediations form.

**NOTE: THESE REPORTS SEARCH THE ENTIRE DATABASE AND ARE NOT LIMITED TO THE ASSESSMENT THE USER IS CURRENTLY VIEWING.

Search Observations and Recommendations / Remediations From Assessment Checklists

This form is used to search all the Observations and Recommendations / Remediations for key words. All assessment facilities in the database are searched using this function.



- The black triangle indicates the record that is selected.

- The fields in the dark green box allow the user to search for and display only the observations and recommendations / remediations of interest.

- The <Search> button performs search based on criteria entered into the fields described above. Key words may be typed into the Facility Name, Observation or Recommendation / remediation fields in the green row. Clicking <Search> will query the entire database for line entries with the key word in the chosen field. Subsequent searches will only be of the previous results unless the <Clear> button is first clicked.

- The <Clear> button will allow all facilities to be seen and searched again.

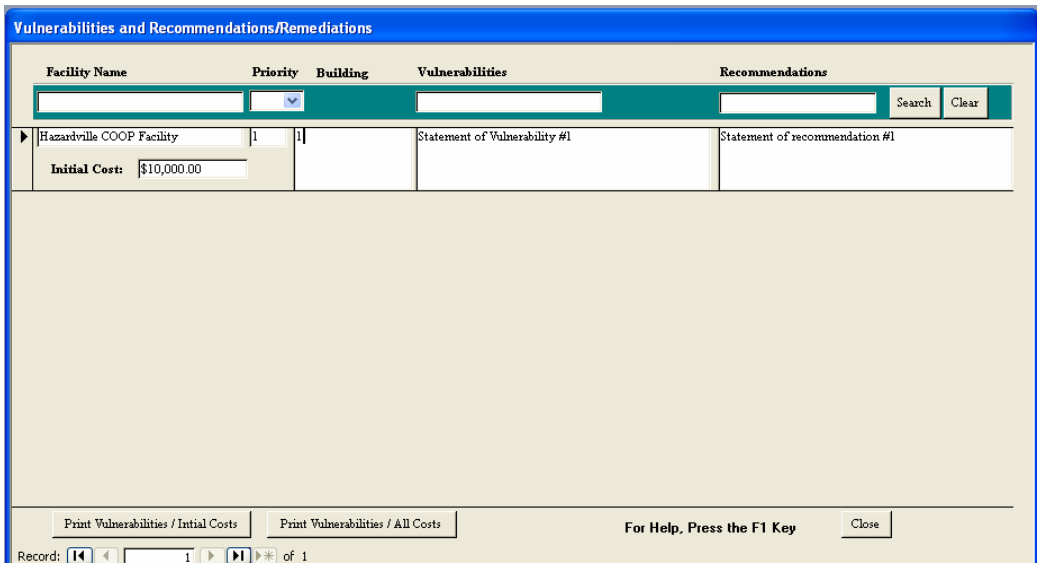
- The <Print, View, Sort by Site> button will create a report of the search results sorted by facility name. The report can be printed or converted to Microsoft Word© and allow additional information to be added, formatting changed, etc.

- The <Print View, Sort by Checklist #> button will create a report of the search results sorted by the question number. The report can be printed or converted to Microsoft Word© and allow additional information to be added, formatted etc.

Click <Close> to return to the previous screen.

Search Vulnerabilities and Recommendations / Remediations

This form is used to search all the Vulnerabilities and Recommendations / Remediations for key words. All the assessment facilities in the database are searched using this function.



- The fields in the green query box allow the user to search for and display only the vulnerabilities and recommendations / remediations of interest.

- The <Search> button performs search based on criteria entered into the fields described above. Key words may be typed into the Facility Name, Observation or Recommendation / remediation fields in the green row. Clicking <Search> will query the entire database for line entries with the key word in the chosen field. Subsequent searches will only be of the previous results unless the <Clear> button is first clicked.

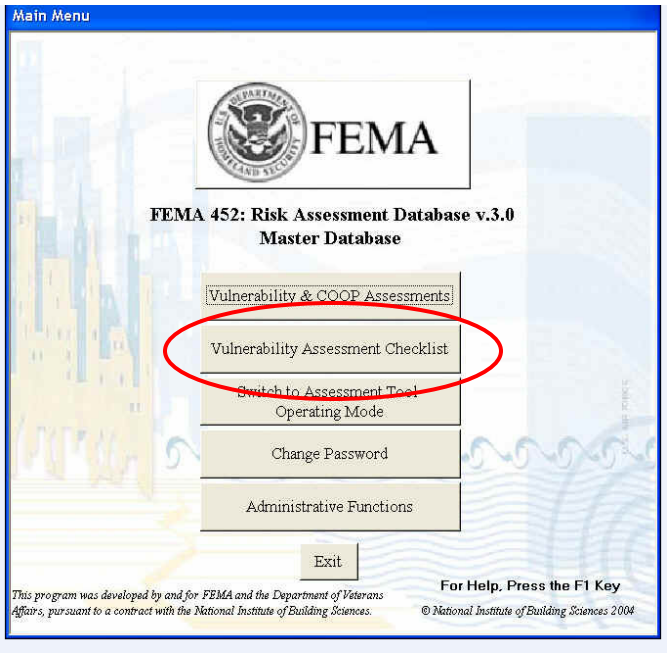
- The <Clear> button will allow all facilities to be seen and searched again.

- The <Print View Vulnerabilities / Initial Costs> button will create a report of the search results sorted by facility name and showing only the initial costs. The <Print View Vulnerabilities / All Costs> button will create a report of the search results sorted by facility name and show all four cost categories. The report can be printed or converted to Microsoft Word© and allow additional information to be added, formatting changed, etc.

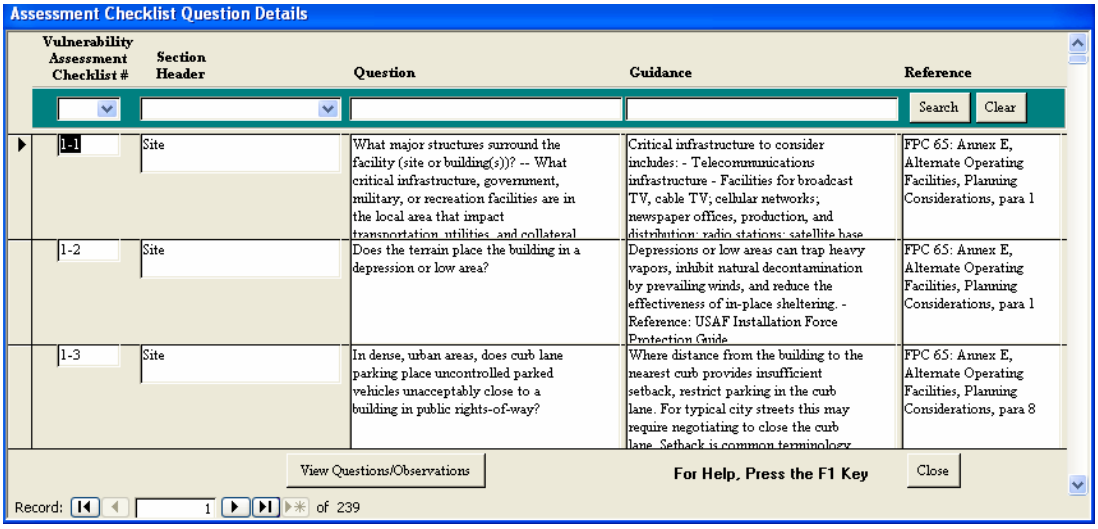
Click <Close> to return to the previous screen.

Vulnerability Assessment Checklist Function

The Vulnerability Assessment Checklist Function gives the Project Manager or an assessor the ability to view all answers for individual checklist questions. To begin this process left click on the <Vulnerability Assessment Checklist> button from the Main Menu.



This form shows all of the assessment checklist questions in the database.



- The black triangle indicates the Checklist Question that is selected.

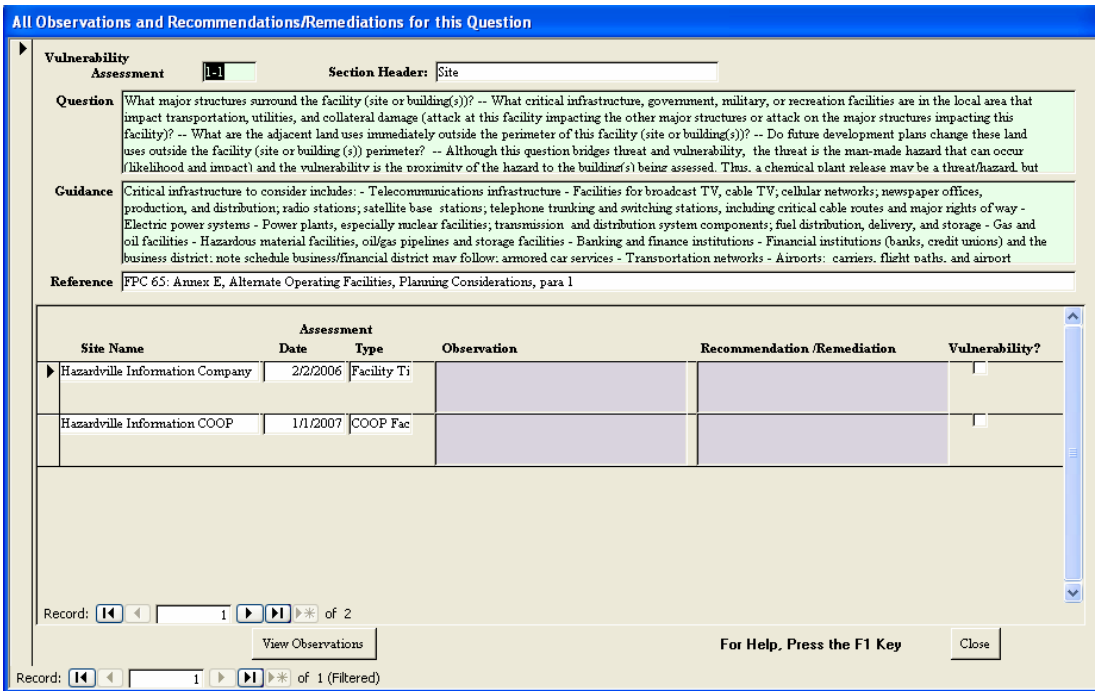
- The green query bar allows the user quick access to the assessment questions by using a drop down menu to select the Checklist section. Keyword searching is also possible, similar to the search routines.

- The <Search> button performs search based on criteria entered into the fields described above. Subsequent searches will only be of the previous results unless the <Clear> button is first clicked.

- The <Clear> button will allow all questions to be seen again.

- The <View Questions/Observations> button opens the All Observations and Recommendations / Remediations for this Question screen based on the selected question.

Observations and Recommendations / Remediations for One Question



This form provides the user with all database entries for the question selected in the Assessment Checklist Question Details form when the <View Questions/Observations> button is selected. The question that is displayed is determined by the location of the arrow in the left column, not by the results of a search that was conducted. It displays the question, guidance, and comments at the top of the form. The bottom of the form displays all information entered in the database for that specific question number.

- The black triangle indicates the record that is selected.

- The <View Observations> button creates a report of all entries in the database for the designated question. The report can be printed or converted to Microsoft Word© for additional editing, formatting, etc.

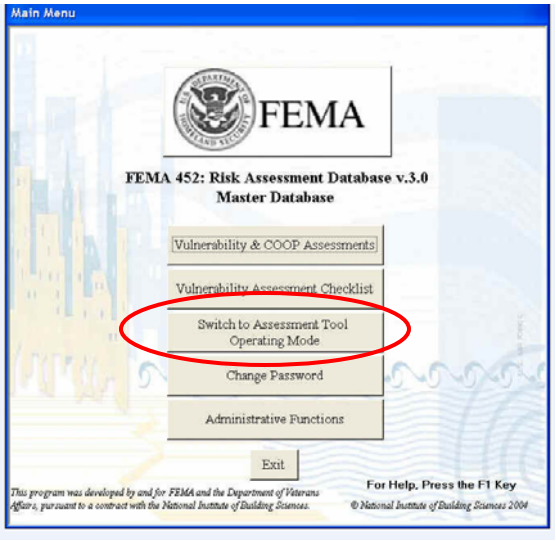
Switching Between Operating Modes

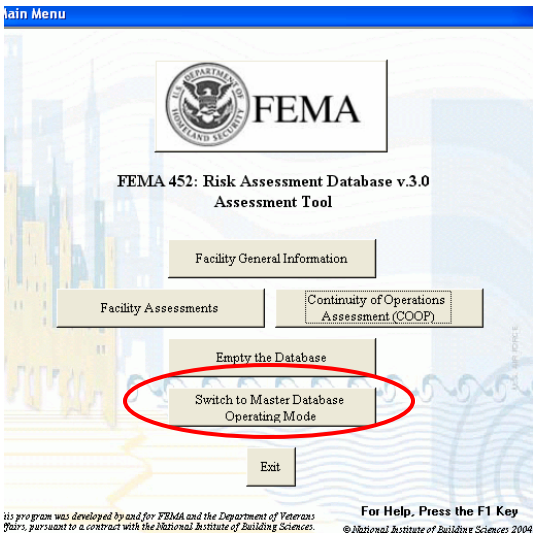
The <Switch Operating Modes> tab takes you between the two operating modes: Assessment Tool mode and Master Database mode.

An organization will generally use two different copies of the database: one loaded on a laptop and operating in the Assessment Tool mode for conducting assessments in the field, and the other loaded on a computer at your organization's headquarters and operating in the Master Database mode for collecting the results from the assessors, printing reports, and archiving the results from a number of assessments. The Master Database copy also provides the organization the ability to search for vulnerabilities common to many assessed facilities, search for specific vulnerabilities, etc. Essentially it can be used as a Risk Management tool to identify and track mitigation measures to reduce risk.

The Assessment Tool mode was designed for engineers and security specialists to be able to easily collect data from the facility being assessed. As you will see, the software is very user friendly. The Master Database mode was designed for the Program Manager.

Switching between the main page of the Assessment Tool to the Master Database mode is as simple as left clicking on the <Switch Operating Modes> button.

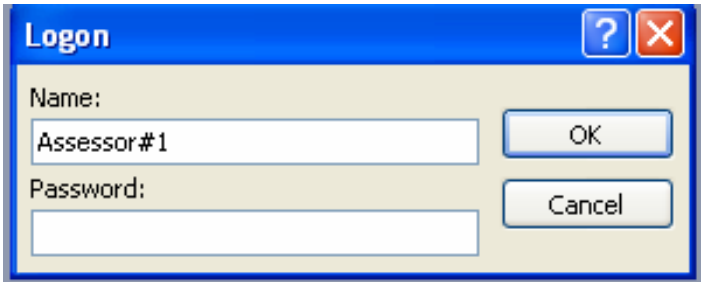




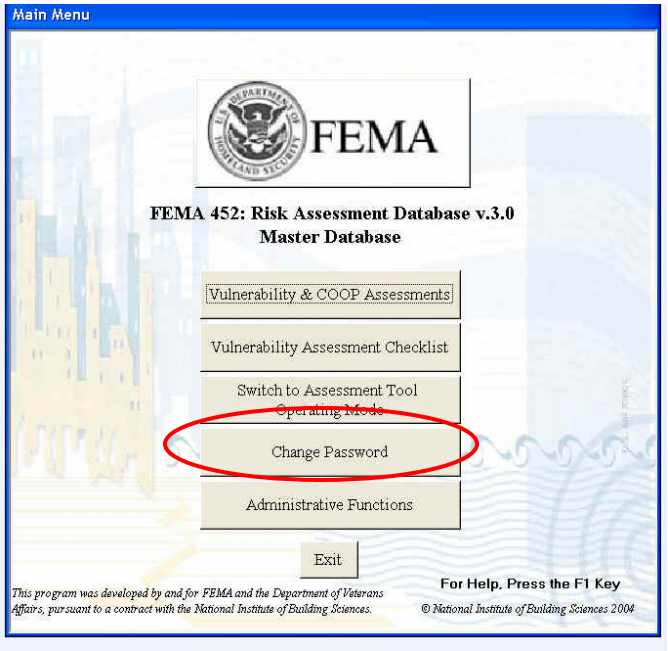
The next window confirms that you want to switch modes. Left click on <Yes> to continue or the other buttons if you do not want to change modes. Then another confirmation window pops up. Left click on <OK>.

Changing Passwords

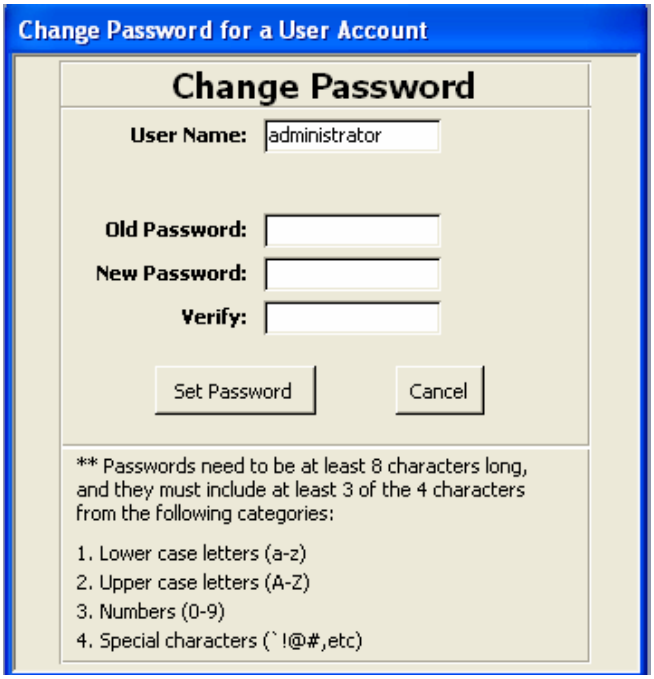
Each user has the ability to change their password from the Master Database operating mode main menu. When a user is initially created by an administrator, their password is blank. To enter the database, simply enter your user name, leave the password field blank, and left click <OK>.



It is highly recommended to change your password at your initial entry into the database. To do this, go to the Main Menu and select <Change Password>.



Selecting the <Change Password > button opens the Change Password Form. Your User name is pre-populated in the top box. Enter your existing password in the "Old Password:" box. Enter a new password in the "New Password:" box. Verify your entry by re-typing the new password in the "Verfy:" box.



Note that password must be eight characters long and they must include at lease three of the four characters from the following categories:

1. Lower case letters (a to z)
2. Upper case letters (A to Z)
3. Numbers (0 to 9)
4. Special characters (`!@#, etc.)

Left click <Set Password> to complete the password change. Left click on <Cancel> to cancel.

Database Administrator Information

Version 3.0 of the FEMA 452 database has simplified the required Database Administrative functions. The Installation Process section of the User Guide describes a step by step process for Users to install and run the database. It simplifies managing user accounts and changing passwords.. It also describes how Users can import database files, Photos, GIS files, and Miscellaneous files.

A Database Administrator may be required to manage the security functions of the database. It is highly recommended that the database administrator is an intermediate to advanced Microsoft Access user. For up to date information about Microsoft Access®, the current software webpage is: http://office.microsoft.com/en-us/FX010857911033.aspx .

Database Specifics:

The database application is composed of various files, including a Microsoft Access© database (*MasterDBV3.mde* for the Master Database), a workgroup file (*FEMA452wg.mdw*), a shortcut to the database (*FEMA Master Assessment Database V3*) *and* a User Guide in Adobe Acrobat © (*FEMA452dB_UserGuide_16-Jan.doc*).

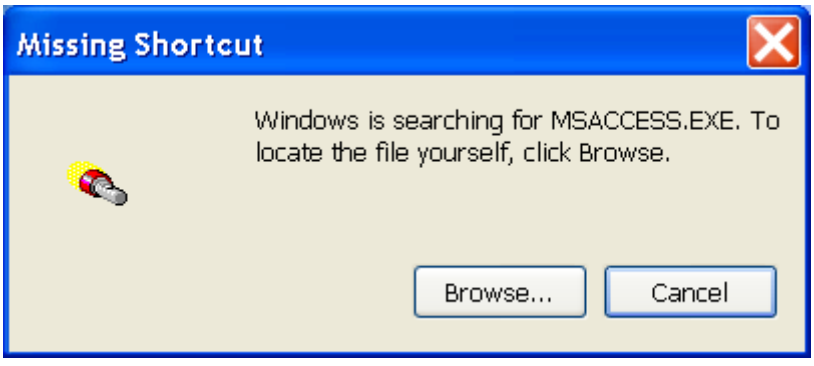
The following are the hardware and software requirements for the risk Assessment Database:

Pentium® 4 or equivalent processor
Windows XP
MS Access© 2002
256 MB of RAM recommended for all components

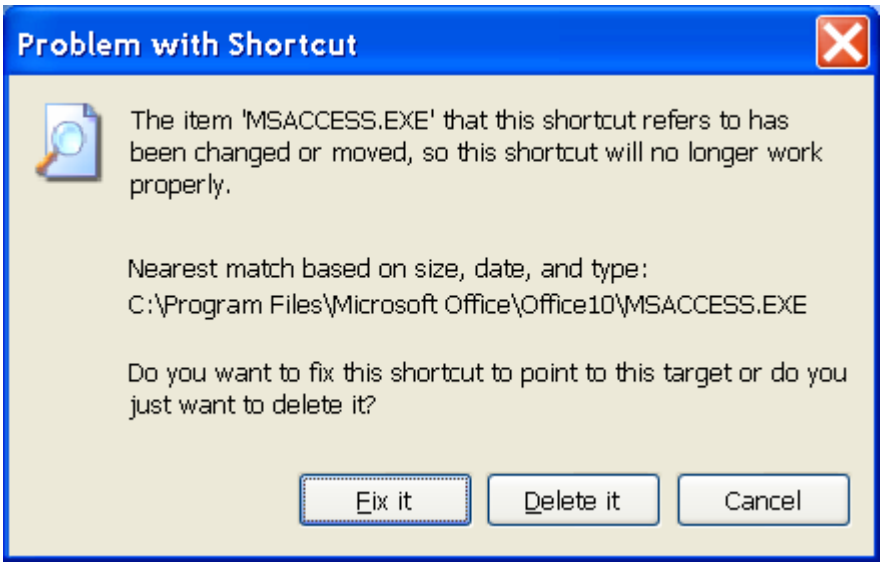
Notes for installation on systems running MS Access© 2002:

(If you are running the program on MS Access© 2003, you will not have this problem.)

The first time the program is started in MS Access© 2002, the below "Missing Shortcut" dialogue box will display.



Simply allow the system to search your system for several minutes until it prompts you with the below “Problem with Shortcut” dialogue box. Then click <Fix it>. This will reset the shortcut to match your system and open the FEMA Master Database program.



Alternately, when you get the first dialogue box, you can browse to your version of MS Access©.

Summary

In this User Guide you have been shown how to install and open the Database. You have also been shown how to link collected data to the databases, how to move around the software and between the Assessment Tool and Master Database, how to handle vulnerabilities, including setting of priorities, and the production of standard reports. Good luck with using the FEMA 452 process and databases in performing a Risk Management Program.