E·GOV

# E-Authentication e-RA Tool Activity Guide

## For use with e-RA Tool v1.5

Version 1.5
October 18, 2005

GSA

# Table of Contents

# 1 e-RA Overview

## *1.1 e-RA Definition*

e-RA is the E-Authentication Risk and Requirements Assessment approach. It is a risk-based technique to elicit authentication requirements for electronic transactions. Its purpose is to guide users in selecting an appropriate level of authentication to resist threats to their data, users, and organizations that could result from unauthorized use of system transactions.

## *1.2 Risk-based Approach*

The e-RA approach emphasizes the development of authentication requirements based on risk. It helps you to identify and assess the risks that can result from unauthorized use of transactions. This helps you identify your true authentication needs and match them to appropriate technical solutions. Viewing authentication purely as a technology issue sometimes causes the deployment of common technology-centric approaches (such as a public key infrastructure) that may not align properly with your authentication requirements. Technology-centric approaches can be:

- more costly than you need
- difficult to implement, manage, and maintain
- a barrier to your intended customers

Using risk to drive the identification of authentication requirements allows you to find and deploy a technical solution that is neither too ineffective nor extensive for your needs.

## *1.3 Authentication Risks*

Improper authentication of users can result in direct and dire consequences to an application. The e-RA approach prompts you to look at your transactions as though **no authentication controls have been implemented.** In this abstract case, e-RA helps you to identify the risks to which the application, its users, and its business partners would be subjected if unauthorized use of transactions occurs. By understanding these risks, you are better able to develop authentication requirements that are based on avoiding the risks unique to your application, rather than accepting a canned technical solution.

Improper authentication can occur in many ways, including:

- a lack of authentication controls
- authentication controls that are inappropriate or weak
- assignment of an inappropriate level of authentication to a user
- poor implementation of authentication controls
- corruption or compromise of authentication controls

e-RA is not, however, a risk assessment methodology for assessing all types of authentication risks. ***e-RA is focused on requirements elicitation, and is not intended as a risk assessment of the operational management of an authentication infrastructure.*** An operational assessment would be better performed as part of a regular risk-based security assessment.

## *1.4 Authentication Levels*

Authentication is a way to ensure that users are who they say they are—that the user who attempts to perform functions in a system is in fact the user who is authorized to do so.

### 1.4.1 Origin of Authentication Levels

For simplicity and consistency, authentication levels are used in e-RA to describe the various degrees of proving the identity of users. The developers of the e-RA approach have included authentication levels that are roughly based on UK standards and consistent with OMB standards[1]. However, users of e-RA can substitute any authentication schema that works for them. The basic e-RA process is flexible and can be matched with a variety of authentication levels.

### 1.4.2 Purpose of Authentication Levels

In e-RA, the authentication levels have two primary purposes:

- to define the characteristics of authentication that a transaction would need to deploy to prevent risks of unauthorized use from being realized
- to provide a foundation for the development of detailed authentication requirements for a set of transactions that can be translated into technical requirements for implementation

Note that the levels do not represent any particular authentication requirements or technical solutions. In the e-RA approach it is important to assign an authentication level to a transaction based on the risks of unauthorized use that have been identified. The authentication level can then be translated to detailed authentication requirements that can be satisfied through technical or operational solutions.

### 1.4.3 Transaction and Data

#### *1.4.3.1 Transactions*

Transactions define the essential activities of a business or organization. They are the primary driver for analysis in the e-RA approach. To determine the best way to authenticate a specific group of users for a transaction, it is important to know the structure and contents of the transaction, who can use it, and what is expected to happen when it is used.

The transactions of a system are the specific actions that users can perform to get a desirable result. In other words a transaction is an actor, plus an action, resulting in a desired outcome. For example, a private citizen (actor) may inquire on government benefit programs (action) to learn about their eligibility (outcome).

#### *1.4.3.2 Transaction Data*

Data is a valuable organizational asset. Depending on its purpose, data may be subject to security requirements such as confidentiality, integrity, and availability.

Transactions are an access path to data. They are the vehicle for creating data, inquiring on it, modifying it, or deleting it. Users utilize transactions to interface with data.

Unauthorized use of transactions permits unauthorized access to data, and potentially violates the data’s security requirements. Transaction-based authentication is one control used to ensure that data, both individual and organizational, is protected from unauthorized actions. Considering the value of data accessed by transactions helps e-RA users to identify the risks of unauthorized use and to choose appropriate authentication levels.

[1] OMB standards are defined in “E-Authentication Guidance for Federal Agencies” issued by the Office of Management and Budget, December 16, 2003. It can be found on-line at www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf. A summary of the authentication levels as defined in these standards is included in Appendix C of this document.

#### 1.4.3.3 Users

Transactions, as defined above, are performed by actors. Individual transactions are associated with individual actors. These actors are the application users that gain access to data and functionality exposed by an application. Considering who should have access to data helps e-RA users to identify the risks associated with an application and to choose an appropriate authentication level.

## 1.5 Primary e-RA Activities

Users perform five primary activities in the e-RA assessment:

- capture application information
- set risk tolerances for their application
- identify the users who have access to the system or application
- identify the transactions of their system or application
- analyze those transactions for risks related to unauthorized use in order to arrive at authentication levels

These activities are described in detail in sections 4 through 13 of this document.

## 1.6 e-RA Results

After using e-RA, a system owner has a mapping of each transaction to an authentication level. These levels can then be used to develop detailed authentication requirements for transactions and to choose and implement technical and other operational solutions for authentication.

# 2 Purpose and Use of the e-RA Tool

The e-RA tool[2] is designed to help users to perform an e-RA. It captures the assessment data and authentication decisions of the application.

Using the tool, Agencies can perform as many assessments as they like, each of which can be identified by assessment date. Over time, the tool can contain all of the assessments performed by an agency and can be consulted for historical or comparison purposes.

A single person or an entire assessment team can use the tool. They may print reports for review or distribution to team members, management, and other stakeholders. Keep in mind that the tool is only a data repository and is not designed to perform analysis of the application's data.

See appendices B and C for more information on using the e-RA tool.

## 2.1 System Requirements

The e-RA tool can be used with Microsoft Access versions 2000 and newer. Older versions of Microsoft Access (i.e., Access 98) will not be able to run this tool.

The tool as delivered is intended for stand-alone use, and should not be implemented in a file-sharing environment with concurrent users.

Because of the size of the input forms in the tool, it is also highly recommended that you set your screen size setting in the Control Panel to no less than 1280 X 1024. This will ensure that you are able to see all relevant input fields and buttons on each form.

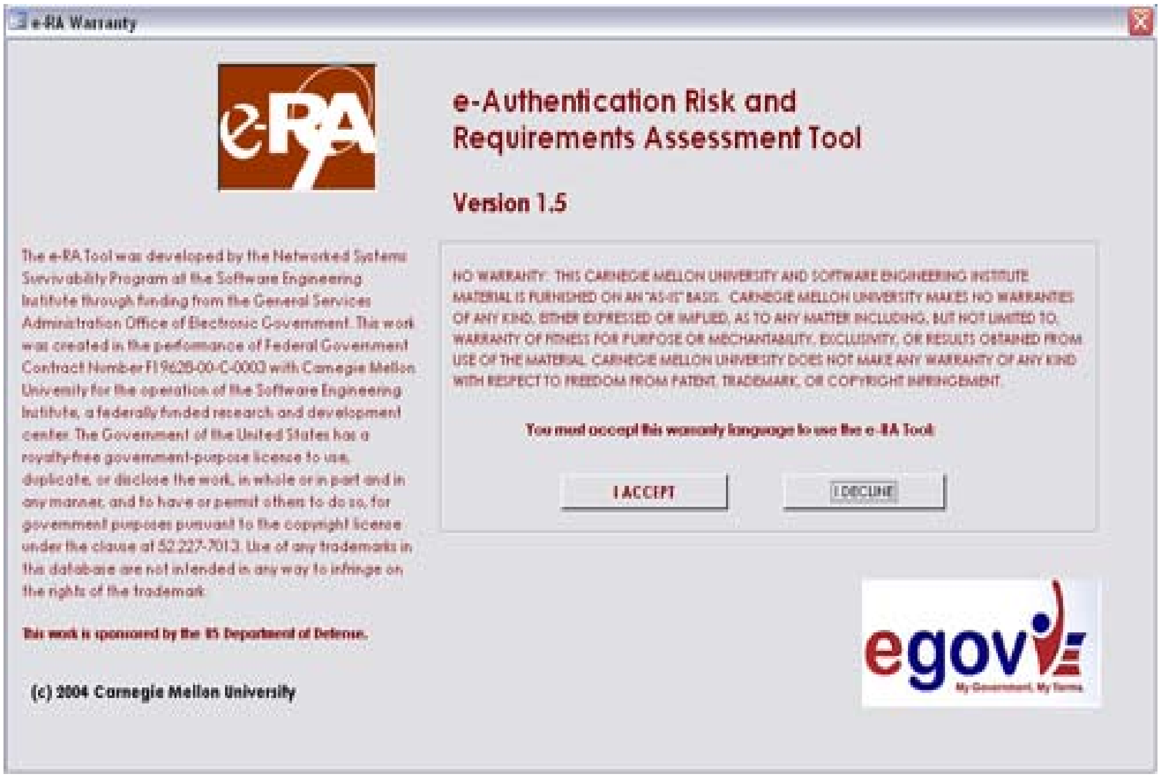
## 2.2 Before Using e-RA

Due to its stand-alone nature, there are some recommended steps that should be followed before using the e-RA tool. First, the user(s) should always make a new copy of the tool prior to beginning. This should be done by simply copying and pasting an empty e-RA database onto the desktop. Second, the new database should be given a meaningful name. It is recommended that the meaningful name use the following naming conventions: "e-RA 1.5 – Application" where the word e-RA does not change, 1.5 signifies the version of the e-RA tool, and Application is a meaningful description of the application going through the e-RA process (e.g. EPA Toxic Sites Application).

[2] The terms "e-RA tool" and "e-RA database" are sometimes used interchangeably in this document. Both refer to the Microsoft Access-based e-RA tool that is used to perform an assessment. This tool can be downloaded at www.cio.gov/eauthentication/era.htm.

## 2.3 Using e-RA Menus

The e-RA tool has a series of menus for ease of navigation. Before accessing the e-RA menu screens, you must accept the warranty language on the screen that appears when you start the e-RA tool.



e-RA Warranty

e-Authentication Risk and Requirements Assessment Tool

Version 1.5

The e-RA Tool was developed by the Networked Systems Survivability Program at the Software Engineering Institute through funding from the General Services Administration Office of Electronic Government. This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose licence to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright licence under the clause at 52.227-7013. Use of any trademarks in this database are not intended in any way to infringe on the rights of the trademark.

This work is sponsored by the US Department of Defense.

(c) 2004 Carnegie Mellon University

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MECHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

You must accept this warranty language to use the e-RA Tool.

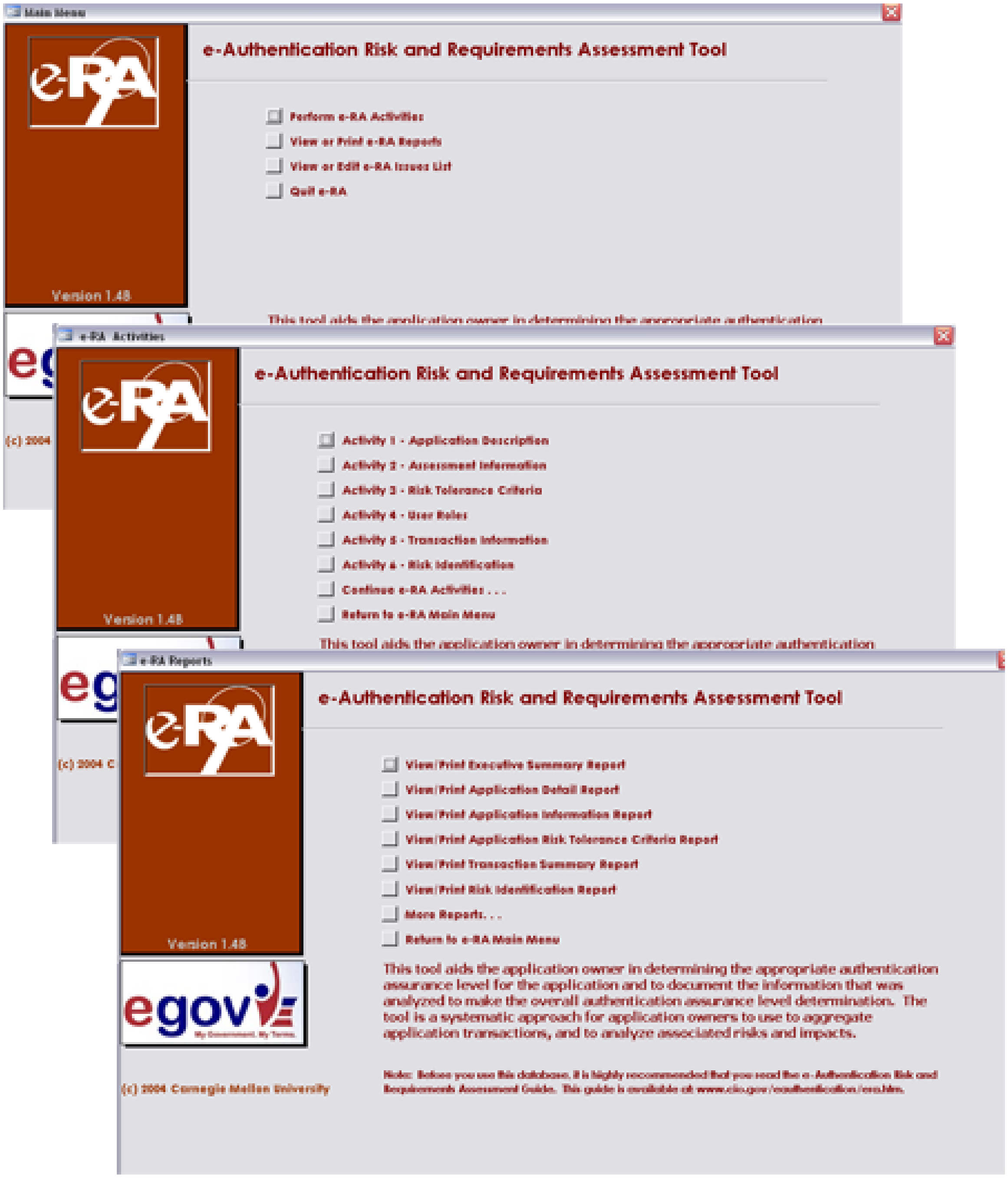
**Figure 1: e-RA Warranty Screen**

If you do not accept the warranty, your e-RA tool session will terminate.

To accept the warranty terms, select the button with text that states “I ACCEPT.” Once you accept the warranty language, you will be directed to the e-RA Menus.

## 2.4 e-RA Menu Layout

Provided below are the three e-RA menu screens.


Main Menu
e-Authentication Risk and Requirements Assessment Tool
e-RA
Version 1.48
□ Perform e-RA Activities
□ View or Print e-RA Reports
□ View or Edit e-RA Issues List
□ Quit e-RA
e-RA Activities
e-Authentication Risk and Requirements Assessment Tool
e-RA
Version 1.48
□ Activity 1 - Application Description
□ Activity 2 - Assessment Information
□ Activity 3 - Risk Tolerance Criteria
□ Activity 4 - User Roles
□ Activity 5 - Transaction Information
□ Activity 6 - Risk Identification
□ Continue e-RA Activities . . .
□ Return to e-RA Main Menu
e-RA Reports
e-Authentication Risk and Requirements Assessment Tool
e-RA
Version 1.48
□ View/Print Executive Summary Report
□ View/Print Application Detail Report
□ View/Print Application Information Report
□ View/Print Application Risk Tolerance Criteria Report
□ View/Print Transaction Summary Report
□ View/Print Risk Identification Report
□ More Reports. . .
□ Return to e-RA Main Menu
egov My Government. My Terms.
(c) 2004 Carnegie Mellon University

This tool aids the application owner in determining the appropriate authentication assurance level for the application and to document the information that was analyzed to make the overall authentication assurance level determination. The tool is a systematic approach for application owners to use to aggregate application transactions, and to analyze associated risks and impacts.

Note: Before you use this database, it is highly recommended that you read the e-Authentication Risk and Requirements Assessment Guide. This guide is available at www.cio.gov/eauthentication/era.htm.

**Figure 2: e-RA Menu Screens**

The first e-RA menu has the four following initial choices to select from:

- Perform e-RA Activities
- View or Print e-RA Reports
- View or Edit e-RA Issues List
- Quit e-RA

When you select an activity on the first menu screen, you will be directed to another menu to navigate through the e-RA tool.

> ⚠ **Some menus continue on subsequent menu screens. Make sure to look for these additional screens where lists of items are continued on another menu.**

Each menu also provides you the ability to navigate back to the first menu or any previous menu.

### 2.4.1 Perform e-RA Activities

This selection directs you to another series of menu items that list all of the e-RA assessment activities. From this screen, you may enter directly into any e-RA activity. Each activity is listed separately and if selected takes the user directly to the input form for that activity.

The e-RA Activities Menu is split into two menu pages. To navigate from one page to another, choose from these selections:

- "Continue e-RA activities . . ."
- "Return to e-RA activities. . ."

### 2.4.2 View or Print e-RA Reports

Almost every activity in the e-RA process has a report associated with it. This selection directs you to a menu that lists all of the e-RA reports.

The e-RA Reports Menu provides direct access to any e-RA report. Each available report is listed separately. Once selected, the report will be presented on the user's screen. You can then print the report by right-clicking and using the Access print options. (**Do not** use the print option on the Access menu—this will print all of the records of the current activity form in which you are working.)

The e-RA Reports Menu is split into two menu pages. To navigate from one page to another, choose the "More reports . . ." and the "Return to e-RA reports. . ." selections.

### 2.4.3 View or Edit Issues List

The e-RA tool has a form for recording any issues, concerns, problems, and action items while performing an assessment. You may access this form directly by selecting this menu item.

### 2.4.4 Quitting e-RA

This selection will close the e-RA tool. When it closes, the tool will save your data and compact and repair the Access database. This will re-organize the data within the database for efficiency upon re-entry.

> ⚠ **If you encounter any problems while entering data in the tool, it is best to quit and restart the tool so that repairs can be made.**

### 2.4.5 Using e-RA Activity Forms

These forms are used for the presentation, entry, and modification of the data collected throughout the e-RA assessment. You may access these forms directly from the e-RA Activities Menu. Or, you may begin with Activity 1 and move to the next activity form by clicking the "Go to Next Activity" button.

⚠ **Forms are not designed to be printed. If you are currently active in a form and you choose "File/Print" from the Access menu bar, be aware that all of the records that have been previously entered in that form will print as well. For example, if you have entered 300 records, all 300 forms will print. Instead, you should view and print e-RA reports rather than forms if you want a printed copy of data that you have entered**.

For new users of Access, more information on using forms and form components is available in Appendix A.

## *2.5 Data Entry and Modification*

### 2.5.1 Data Entry

Forms allow you to enter and modify data for your e-RA assessment. Once data is entered and saved, you can then use the buttons to navigate through this data and to modify it as necessary. You will begin the data entry process with the first form/activity, "Application Description," and end with the checklist in "Next Steps."

### 2.5.2 Data Modification

Once you have entered data into the e-RA tool, you have the ability to modify this information. Keep in mind the following points when modifying data:

- Use the navigation buttons to search for the data that you want to modify.
- Changes and deletions will modify or eliminate all associated data.

# 3 Inputs to e-RA

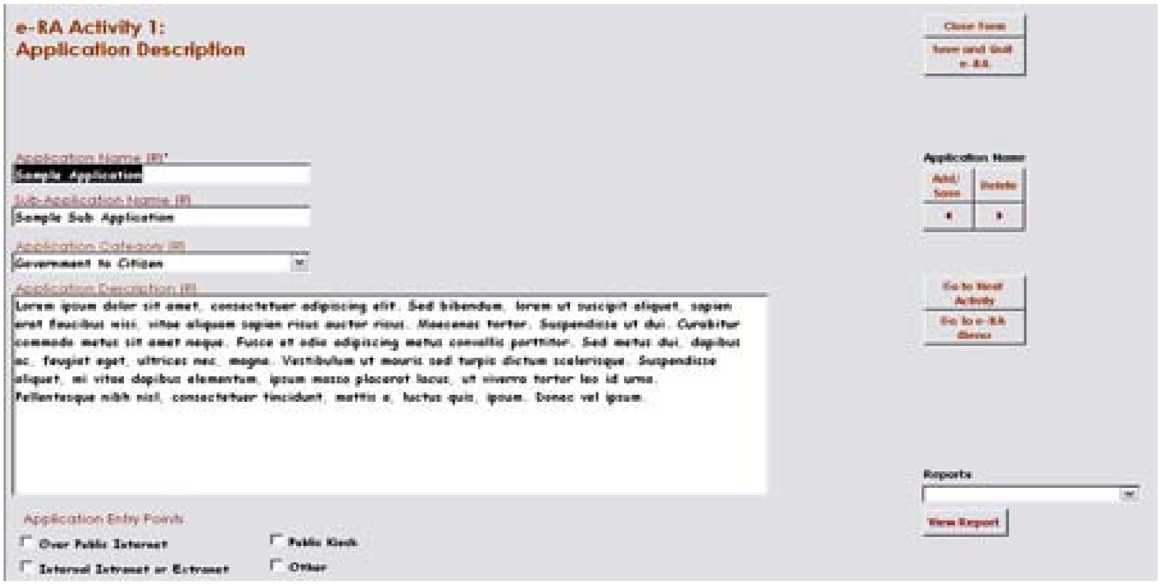
To get started with an e-RA assessment, you will need the following:

- OMB guidance on authentication levels, currently available at www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf or another set of authentication levels you wish to use
- Knowledgeable participants. Generally, 1-5 people perform e-RA. They must be able to describe the transactions of the application and to identify and analyze the consequences of unauthorized use. It may also be helpful if the participants have access to others in the agency or the sponsoring organization to contribute to or validate some decisions and outputs of e-RA.
- Application business case
- List of application transactions
- e-RA tool

Once you have assembled these, open the e-RA tool in Microsoft Access and begin.

# 4 e-RA Application Description

Provided below is the e-RA screen used to complete Activity 1 – Application Description.



e-RA Activity 1:
Application Description

Application Name (R)*
Sample Application

Sub-Application Name (R)
Sample Sub Application

Application Category (R)
Government to Citizen

Application Description (R)
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Sed bibendum, lorem ut suscipit aliquet, sapien erat faucibus nisi, vitae aliquam sapien risus auctor risus. Maecenas tortor. Suspendisse ut dui. Curabitur commodo metus sit amet neque. Fusce et odio adipiscing metus convallis porttitor. Sed metus dui, dapibus ac, feugiat eget, ultrices nec, magna. Vestibulum ut mauris sed turpis dictum scelerisque. Suspendisse aliquet, mi vitae dapibus elementum, ipsum massa placerat lacus, ut viverra tortor leo id urna. Pellentesque nibh nisl, consectetuer tincidunt, mattis a, luctus quis, ipsum. Donec vel ipsum.

Application Entry Points
☐ Over Public Internet
☐ Internal Intranet or Extranet
☐ Public Kiosk
☐ Other

**Figure 3: Activity 1 – Application Description**

## 4.1 Purpose

The purpose of this activity is to record the basic information about an application.

## 4.2 Background

Although the information here is not used directly in any subsequent step of e-RA, it provides context.

For more background information, see **Concepts** (below).

## 4.3 Important Tips

**Caution**: Don't advance through the white fields until you have entered data in the check boxes. Otherwise, you will have to go back and edit this form.

## 4.4 Performing the Activity

Use the following steps to complete Activity 1 – Application Description:

1. Record the application name.

2. Record the sub-application name, if applicable.

3. Select the category of application.

4. Describe the application.

5. Select points of entry where users can access the application.

6. Click on the “Add/Save” button to save your work. You will see a blank screen. You can enter another application or continue to step 7.

7. Click on the “Go to Next Activity” button.

## 4.5 Other Issues

At any time, you may click the button labeled “Record an Issue” to go to a form for capturing issues and concerns that arise during the assessment.

The application can then direct further attention to these issues after the e-RA assessment or as a part of a regular risk assessment activity performed on the application.

## 4.6 Concepts

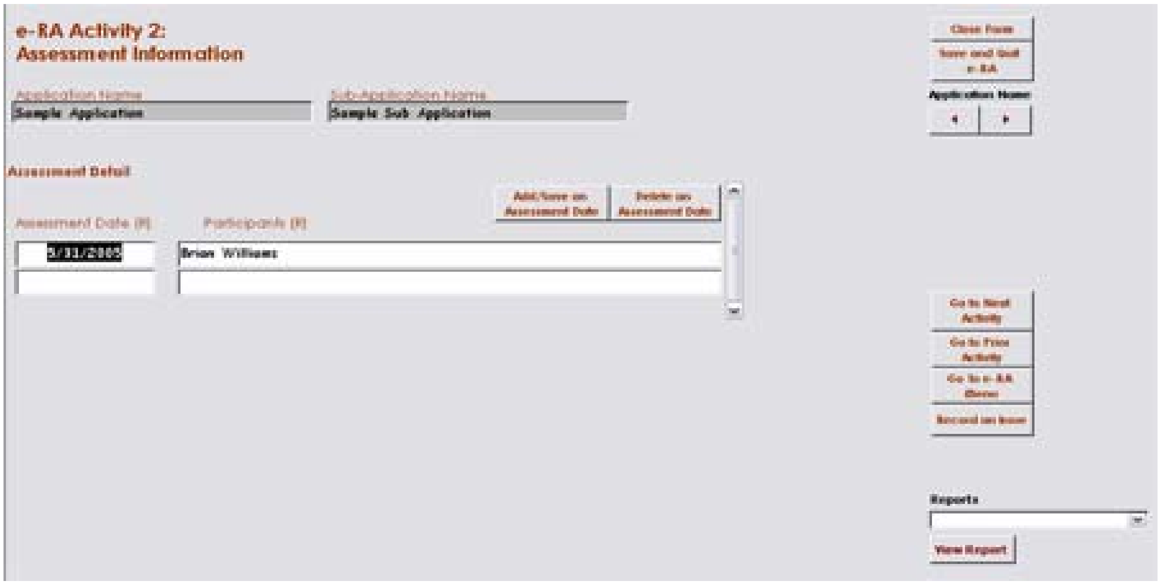
The purpose of this activity is to elicit a brief description of the application’s mission or business case and the status of the development effort, if known.

e-RA participants describe the core services to be provided through the application, gather sufficient detail to describe the boundaries of the application’s services, and concentrate on identifying the extent to which the business processes and the structure (i.e., application and technical infrastructure) of the application have been defined. If the application has not been completely defined, focus the remainder of the e-RA activities on the proposed definition of the business processes and transactions.

You do not gather specific transaction detail in this activity. Rather, capture a general sense of the application’s core mission so that this can be used as the context going forward in the assessment.

# 5 e-RA Assessment Information

Provided below is the e-RA screen used to complete Activity 2 – Assessment Information.



Application Name: Sample Application

Sub-Application Name: Sample Sub Application

| Assessment Date (R) | Participants (R) |
|---|---|
| 3/31/2005 | Brian Williams |
| | |

**Figure 4: Activity 2 – Assessment Information**

## 5.1 Purpose

The purpose of this activity is to document the assessment date and the participants who performed the assessment.

## 5.2 Background

The e-RA tool distinguishes each assessment by date. You may perform more than one assessment on an application. As conditions change, this also allows you to go back and review or update prior assessments.

## 5.3 Important Tips

**Caution:** If you delete an assessment date, all data associated with this date throughout the e-RA tool will be deleted.

## 5.4 Performing the Activity

Use the following steps to complete Activity 2 – Assessment Information:

1. Check the shaded boxes at the top of the form to ensure that the name of the application (and sub-application, if applicable) is correct.

2. Fill in the date box.

3. List the participants' names, separated by commas.

4. Click on the "Add/Save an Assessment Date" button.

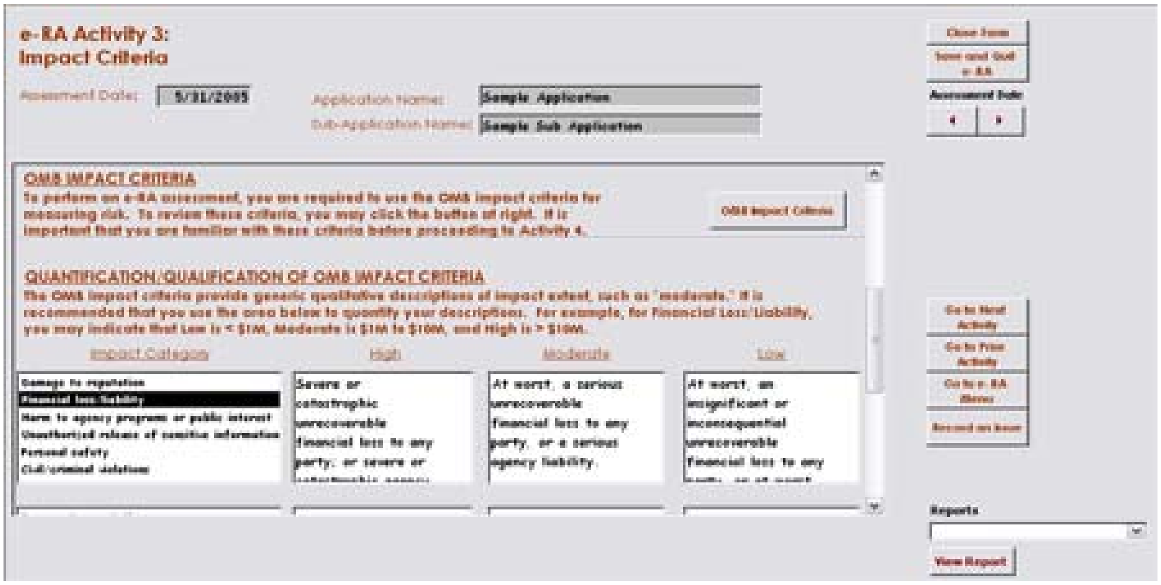
5. Click on the “Go to Next Activity” button.

## 5.5 Other Issues

At any time, you may click the button labeled “Record an Issue” to go to a form for capturing issues and concerns that arise during the assessment.

# 6 e-RA Risk-Tolerance (Impact) Criteria

Provided below is the e-RA screen used to complete Activity 3 – Risk-Tolerance (Impact) Criteria.



e-RA Activity 3:
Impact Criteria

Assessment Date: 5/31/2005

Application Name: Sample Application

Sub-Application Name: Sample Sub Application

OMB IMPACT CRITERIA

To perform an e-RA assessment, you are required to use the OMB impact criteria for measuring risk. To review these criteria, you may click the button at right. It is important that you are familiar with these criteria before proceeding to Activity 4.

QUANTIFICATION/QUALIFICATION OF OMB IMPACT CRITERIA

The OMB impact criteria provide generic qualitative descriptions of impact extent, such as "moderate." It is recommended that you use the area below to quantify your descriptions. For example, for Financial Loss/Liability, you may indicate that Low is < $1M, Moderate is $1M to $10M, and High is > $10M.

| Impact Category | High | Moderate | Low |
|---|---|---|---|
| Damage to reputation<br>Financial loss/liability<br>Harm to agency programs or public interest<br>Unauthorized release of sensitive information<br>Personal safety<br>Civil/criminal violations | Severe or catastrophic unrecoverable financial loss to any party; or severe or | At worst, a serious unrecoverable financial loss to any party, or a serious agency liability. | At worst, an insignificant or inconsequential unrecoverable financial loss to any |

**Figure 5: Activity 3 – Risk-Tolerance (Impact) Criteria**

## 6.1 Purpose

The purpose of this activity is to set the risk-tolerance or impact criteria for your application.

## 6.2 Background

The set of risk-tolerance criteria that you use serves as a benchmark, specific to your organization, for measuring the impacts of unauthorized use of transactions. **In the case of E-Government applications, these criteria have been developed for you by OMB.**

For more background information, see **Concepts** (below).

## 6.3 Important Tips

Always check the top portion of any form that you are working in to see that you are on the correct assessment by date.

You may need input from others in your organization or application in order to develop meaningful risk tolerance criteria.

You will find the OMB impact criteria on the activity form for your reference. Click on the "OMB Impact Criteria" button to review. You may also click on the report button "OMB Impact Criteria" if you want to print a copy of these criteria for later use.

## 6.4 Performing the Activity

Use the following steps to complete Activity 3 – Risk-Tolerance (Impact) Criteria:

1. Check the shaded boxes at the top of the form to ensure that the name of the application (and sub-application, if applicable) is correct.

2. Click on the “OMB Impact Criteria” to review the standard criteria that OMB has provided in authentication guidance for E-Government applications.

3. If you would like to add qualification to the OMB guidance for your application (either quantitative or qualitative), choose the appropriate impact category that you want to qualify and then record your qualifications for high, moderate, or low impacts. For example, where an OMB criterion specifies “substantial financial loss,” you may want to quantify that loss for your application to be “greater than $1,000,000.” Click the “Add/Save Criteria” button to record your qualification.

4. Continue with the next impact category until you have provided qualifications for each impact category as desired. Remember to click the “Add/Save Criteria” button each time you record a qualification for an impact category.

5. Click on the “Go to Next Activity” button.

## *6.5 Other Issues*

At any time, you may click the button labeled “Record an Issue” to go to a form for capturing issues and concerns that arise during the assessment.

## *6.6 Concepts*

### 6.6.1 Impact

Risk-tolerance criteria are developed to provide a specific way to measure the extent to which the application is affected by the consequences of unauthorized use of a transaction. The effect on the organization is defined as an “impact.”

### 6.6.2 Risk-Tolerance or Impact Criteria

Risk tolerance criteria are benchmarks or measures against which the organization can evaluate the impacts of unauthorized use of an application’s transactions. The risk-tolerance criteria reflect the organization’s specific tolerance for risks.

If you are an E-Government application, you are required to use the OMB impact categories as they are provided in the e-Authentication Guidance for Federal Agencies, section 2.2.

In the e-RA approach, the risk-tolerance criteria embody three principles:

1. Because each organization has different drivers, the risk-tolerance criteria for each organization may be different. In essence, the organization develops its own weighting factors to describe what is important, rather than accepting these factors from external parties. (When using the OMB impact categories, this weighting is performed by qualifying the criteria either qualitatively or quantitatively).

2. Risk-tolerance criteria are important for determining the appropriate type and extent of authentication controls that would prevent the impacts related to the unauthorized use of transactions.

3. The risk-tolerance criteria allow an application to determine the relative severity of a particular impact and to identify those impacts that the organization most wants to avoid. The relative severity is a qualitative measurement, described as high, moderate, or low. For example, the effects of a financial fraud resulting from unauthorized use of a transaction will vary depending on the organization. If the fraud results in a $10 million loss, this may be a high impact to one organization and a low impact to another. The risk tolerance criteria are organization-specific to allow for these variations.

### 6.6.3 Impact Categories

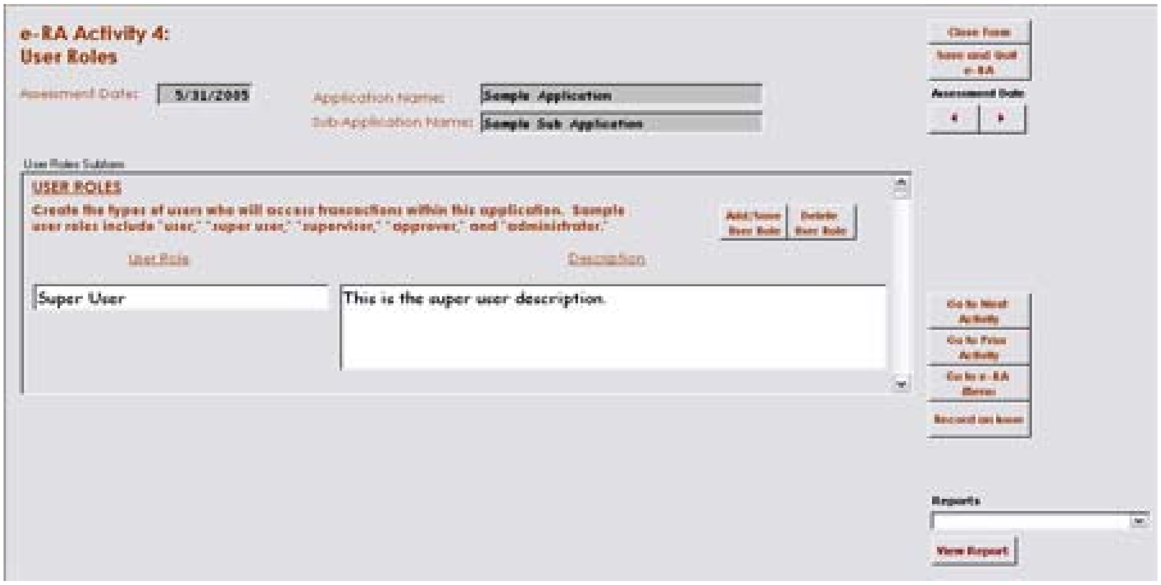
Risk tolerance criteria can be categorized or arranged by the type of impact that they describe. These categories are referred to as impact categories. OMB provides six standard impact categories and corresponding criteria:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs of public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

When the consequences of unauthorized use of transactions are realized by the organization, these impact categories can be used to measure the extent of the effect on the organization.

# 7 e-RA User Roles

Provided below is the e-RA screen used to complete Activity 4 – User Roles.



e-RA Activity 4:
User Roles

Assessment Date: 5/31/2005

Application Name: Sample Application

Sub-Application Name: Sample Sub Application

User Roles Subform

USER ROLES

Create the types of users who will access transactions within this application. Sample user roles include "user," "super user," "supervisor," "approver," and "administrator."

| User Role | Description |
|---|---|
| Super User | This is the super user description. |

**Figure 6: Activity 4 – User Roles**

## *7.1 Purpose*

The purpose of this activity is to identify the set of user roles that will be assessed using the e-RA approach.

## *7.2 Background*

User roles are representations of the people who will have access to the application through transactions. You may assess as many user roles as you like. For more background information, see **Concepts** (below).

## *7.3 Important Tips*

Always check the top portion of any form that you are working in to see that you are on the correct assessment by date.

**Caution**: Don't advance through the white fields until you have entered data in the check boxes. Otherwise, you will have to go back and edit this form.

## *7.4 Performing the Activity*

Use the following steps to complete Activity 4 – User Roles:

1. Check the shaded boxes at the top of the form to ensure that the date and name of the application (and sub-application, if applicable) is correct.

2. Fill in the user role name.

3. Record a user role description. Write as much as you like to be clear in describing the user role.

4. Click on the "Add/Save User Role" button. This will save the current user role and provide a clean form to record additional user roles.

5. Click on the "Go to Next Activity" button.

## *7.5 Other Issues*

At any time, you may click the button labeled "Record an Issue" to go to a form for capturing issues and concerns that arise during the assessment.

## *7.6 Concepts*

### 7.6.1 User Roles

While transactions are the primary driver for analysis in the e-RA approach, user roles are the primary driver for our understanding of a transaction. To determine the best way to authenticate a specific group of users for a transaction, it is necessary to understand who those users are and what transactions they will be able to perform.

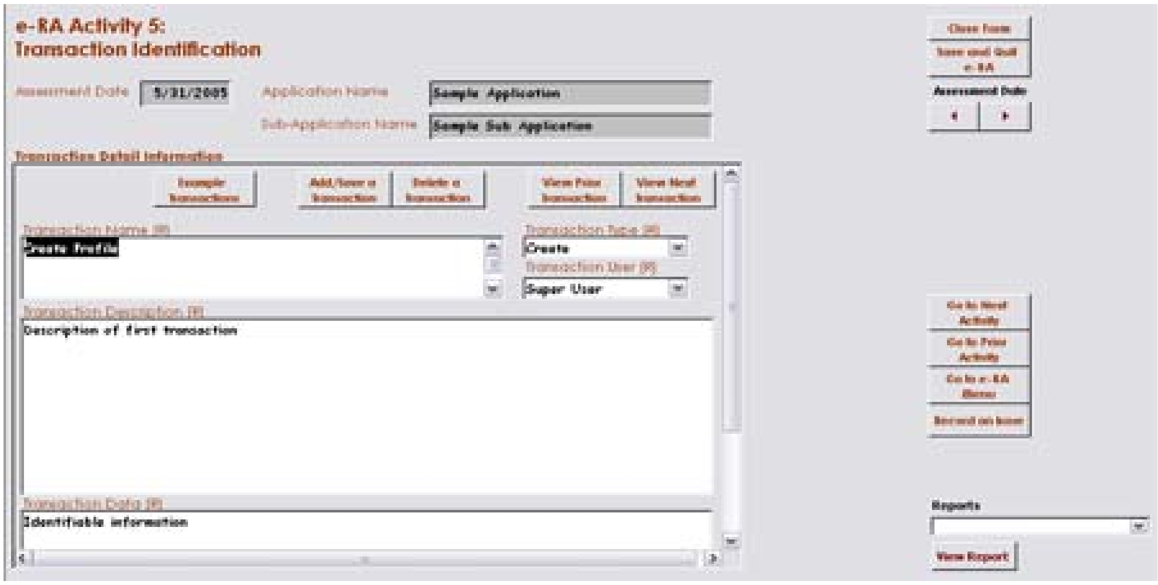
Some sample user roles include Administrator, Super User, User, Approver, and Supervisor.

### 7.6.2 User Roles to Include in the Assessment

User roles will be assigned individual assurance level requirements. For this reason, it is imperative that all user roles be represented in the e-RA. In subsequent steps, it will also be important to make that there are enough user role specific transactions to provide a full understanding of the user roles assurance level needs.

# 8 e-RA Transaction Identification

Provided below is the e-RA screen used to complete Activity 5 – Transaction Identification.



e-RA Activity 5:
Transaction Identification

Assessment Date: 5/31/2005

Application Name: Sample Application

Sub-Application Name: Sample Sub Application

Transaction Detail Information

Transaction Name (R): Create Profile

Transaction Type (R): Create

Transaction User (R): Super User

Transaction Description (R): Description of first transaction

Transaction Data (R): Identifiable information

Figure 7: Activity 5 – Transaction Identification

## 8.1 Purpose

The purpose of this activity is to identify the set of transactions that will be assessed using the e-RA approach.

## 8.2 Background

Transactions form the basis for the e-RA approach. You may assess as many transactions as you like. Some applications only assess a subset of transactions from their application. If you decide to use a subset, make sure they are a representative sample. For more background information, see **Concepts** (below).

## 8.3 Important Tips

Always check the top portion of any form that you are working in to see that you are on the correct assessment by date.

**Caution:** If you delete a transaction, all data associated with this transaction throughout the e-RA tool will be deleted.

**Caution**: Do not advance through the white fields until you have entered data in the check boxes. Otherwise, you will have to go back and edit this form.

## *8.4 Performing the Activity*

Use the following steps to complete Activity 5 – Transaction Identification:

1. Check the shaded boxes at the top of the form to ensure that the date and name of the application (and sub-application, if applicable) is correct.

2. Fill in the transaction name.

3. Select a transaction type.

4. Select a transaction user.

5. Record a transaction description. Write as much as you like to be clear in describing the transaction.

6. Describe the data associated with this transaction. Note any special restrictions on this data or indicators of sensitivity. You may also indicate any security requirements associated with the data (confidentiality, integrity, or availability).

7. If this transaction requires non-repudiation, check the box next to the statement, “Transaction Requires Non Repudiation.”

8. Click on the “Add/Save a Transaction” button. This will save the current transaction and provide a clean form to record additional transactions.

9. Click on the “Go to Next Activity” button.

## *8.5 Other Issues*

At any time, you may click the button labeled “Record an Issue” to go to a form for capturing issues and concerns that arise during the assessment.

## *8.6 Concepts*

### 8.6.1 Transaction-based Assessment

Transactions are the primary driver for analysis in the e-RA approach. To determine the best way to authenticate a specific group of users for a transaction, it is important to know the structure of the transaction, who can use it, and what is expected to happen when it is used.

The transactions in an E-Government application define the specific activities that are desired to meet the application’s goals and objectives. For example, the ability for a private citizen to inquire on benefit programs that fit their individual needs could be a primary objective of an online eligibility assistance application. This transaction is meant to be used by a specific group of users and the desired outcomes (i.e., a private citizen gets valuable information on government benefit programs) have been established.

For some applications, a complete set of transactions for the application will be analyzed. For others, the transactions will be a **representative set**. Identifying the appropriate transactions depends on a number of factors, including the business purpose of the application, the current or expected logical and physical designs for the application’s systems, and the boundaries of the application.

### 8.6.2 Transactions to Include in the Assessment

Understanding the criticality, volume, and range of transactions that the application offers will help to define authentication needs. Pilots of e-RA demonstrated that five to seven transactions are sufficient to successfully define authentication needs. If you are using a subset of transactions to define authentication requirements, consider the categories below to help you decide how to choose which transactions to analyze:

- Critical transactions – those most relevant to the purpose or mission, or without which the application could not fulfill its primary objectives. These transactions reveal the core of the services provided by the application and are those that need the most scrutiny.
- Common transactions – transactions that are used most frequently. Because they are used often, these transactions provide a greater possibility of misuse. There may be some overlap between common and critical transactions.
- Unique transactions – those that are neither common nor ordinary and that may have a special purpose or distinctive users.
- Range of transactions – the range of transactions defines the upper and lower limits of the transactions in terms of what they allow users to do, and that all types of transactions are covered
- Range of users – all user roles previously defined in e-RA need to have sufficient transactions to determine an authentication level specific to that user.

### 8.6.3 Transaction Types

The risk assessment techniques for identifying the consequences of unauthorized use of transactions are highly dependent on the transaction type. Thus, each transaction that is assessed in the e-RA approach must be categorized in one of four types: inquire, create, modify, or delete. Each of these types is described below:

- Inquire – this transaction allows the user to access data or information. The user makes a request for information and receives it. This information may be related to the user in some way (i.e., private) or can be general information (i.e., public.).
- Create – this transaction allows the user to put new data or information in a system. The user creates new data that does not currently exist. However, if existing information is available in a system and new information is appended, the “create” transaction is essentially a modification of existing data, and is covered by the “modify” transaction.
- Modify – this transaction allows the user to modify existing data or information in a system and save those changes. The original information may or may not be recoverable.
- Delete – this transaction allows the user to destroy or eliminate data or information so that it is no longer available for inquiry or modification. The elimination of data or information may be temporary (recoverable) or permanent (unrecoverable.)

There are variations on these categories and you may also have some unique variations to describe. For example, “approve” may be a transaction in which a request or voucher is approved by an appropriate party. In the e-RA approach, this transaction is a form of a “modify” transaction because it appends additional data to the existing record. In addition, a “cancel” transaction could be classified as a type of “delete” in which an action or approval is voided. The original request or authorization may still be kept for historical purposes. You must be sure to thoroughly analyze the action of the transaction to properly categorize it. This may require you to describe unique situations in sufficient detail to ensure proper categorization.

### 8.6.4 Transaction Data

Transactions are the gateway to a system's data or information. Providing access to use a particular transaction essentially provides access to the transaction's data. Implementing authentication controls to ensure that transactions are used only by authorized users is one way to protect data from unauthorized access.

You must consider a transaction's data in order to identify risks associated with unauthorized use of a transaction. For example, a transaction that permits a user to inquire on public information or data may not result in any risk because the data or information does not specifically need to be protected. However, if the inquiry is on private data, many risks may result because of the potential unauthorized disclosure of private data.

For each transaction, you should specifically identify the data associated with the transaction. You should consider and document the following:

- whether the data's use will be restricted only to certain actors or groups of actors
- if the data must be available for use by the actors for any critical timeframe
- if the data is private, sensitive, or otherwise requiring a high level of protection

You may also want to note if the data has any specific information security requirements such as confidentiality, integrity, or availability. If so, these requirements should be considered when identifying the consequences of unauthorized use of transactions that access this data.

### 8.6.5 Other Transaction Information

You may want to record other information on transactions when defining them if that information is relevant to authentication needs. For example

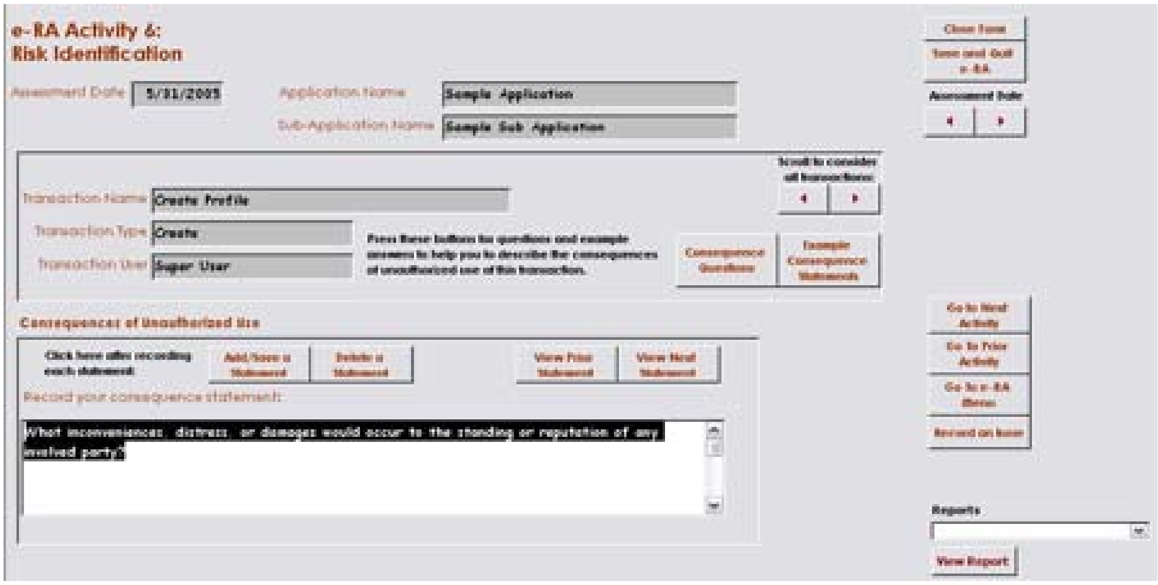
- the flow of transactions (for example, a "create" must precede an "approval")
- unusual aspects of a transaction (for example, a "delete" transaction doesn't actually remove a record)
- the expected volume of the transaction
- triggered transactions or activities that occur when the transaction being reviewed is executed

### 8.6.6 Non-repudiation

Non-repudiation is sometimes referred to as a business requirement rather than a security requirement. Either way, it is relevant to authentication. A non-repudiation requirement binds a user to an action (such as the use of a transaction) in a way that the user cannot refute (or repudiate) their intent to be bound.

# 9 e-RA Risk Identification

Provided below is the e-RA screen used to complete Activity 6 – Risk Identification.



e-RA Activity 6:
Risk Identification

Assessment Date: 5/31/2005

Application Name: Sample Application

Sub-Application Name: Sample Sub Application

Transaction Name: Create Profile

Transaction Type: Create

Transaction User: Super User

Press these buttons for questions and example answers to help you to describe the consequences of unauthorized use of this transaction.

Consequences of Unauthorized Use

Click here after recording each statement:

Record your consequence statement:

What inconveniences, distress, or damages would occur to the standing or reputation of any involved party?

**Figure 8: Activity 6 – Risk Identification**

## 9.1 Purpose

The purpose of this activity is to identify the consequences of unauthorized use of transactions.

## 9.2 Background

The threat of unauthorized use plus the resulting consequence of that action define a risk. For more background information, see **Concepts** (below).

## 9.3 Important Tips

Always check the top portion of any form that you are working in to see that you are on the correct assessment by date.

You will perform risk identification activities on **one transaction at a time** on this form. You should periodically check to ensure that you are working on the intended transaction.
This form provides a single response block to record consequence statements. You can record as many consequence statements as necessary, but you should avoid combining them into a single response. Use a blank form for each consequence statement.

The e-RA tool includes lists of questions and example answers to prompt you to think about the consequences of unauthorized use. It is highly recommended that you use these questions to elicit consequence statements. If you use these questions, you do not need to answer every question. Conversely, you may identify many consequences in response to a single question that is particularly relevant for you. These questions will be pre-populated for each transaction in the e-RA tool.

## *9.4 Performing the Activity*

Use the following steps to complete Activity 6 – Risk Identification:

1. Check the shaded boxes at the top of the form to ensure that the date and name of the application (and sub-application, if applicable) is correct.

2. Check the Transaction Name, Transaction Type, and Transaction User boxes to confirm that you are assessing the intended transaction.

3. Click on the button labeled “Consequence Questions” to get a list of questions to help you develop statements that describe the consequences of unauthorized use of the transaction. Click on the button labeled “Example Consequence Statements” to see examples. You may print these lists for reference.

4. Record each consequence statement separately in the white box labeled “Record Your Consequence Statement”. Write as much as you like to express that consequence. Put only one consequence in this box.

5. Click on the button labeled “Add/Save a Statement” to save that statement and get a blank form for the next statement.

6. Repeat steps 4 and 5 until you have recorded all the consequence statements for that transaction.

7. Click on the arrow buttons next to “Scroll to consider all transactions” to advance to the next transaction or move to prior transactions to revise.

8. Repeat steps 2 through 7 until you have recorded all of the consequence statements for each of your transactions.

9. Click on the “Go to Next Activity” button.

## *9.5 Other Issues*

At any time, you may click the button labeled “Record an Issue” to go to a form for capturing issues and concerns that arise during the assessment.

## *9.6 Concepts*

### 9.6.1 Consequences of Unauthorized Use

A primary objective of the e-RA approach is to identify the consequences of unauthorized use of transactions, and the authentication controls necessary to prevent these consequences. The threat of unauthorized use of a transaction and the potential consequences constitutes a risk for the application.

In the risk identification activity, you develop and document the consequences of unauthorized use for each transaction that you are assessing. This is performed by answering a series of questions that help you to draw out consequence statements depending on the type of transaction you are assessing. The type of transaction (i.e., inquire, etc.) is important for developing these consequence statements because each type affects data in different ways.

For example, when an authorized user inquires on a payroll record, the desired outcome is that the authorized user (the owner of the record or their authorized agent) is able to view this information. Conversely, when an unauthorized user executes this inquiry, undesired outcomes occur, such as disclosure of personal information to other than the owner of the information. These undesired outcomes from unauthorized use of transactions present potential consequences to the application.

### 9.6.2 Transaction Types and Consequences

Depending on the type of transaction, unauthorized use can result in many possible undesired outcomes and consequences to the application. This is because of the inherent effect that each transaction has on related data and information.

You should consider these effects when determining the consequences of unauthorized use of a transaction. For example:

- *Inquire* transactions generally provide access to view data. Unauthorized use can result in disclosure of data to users other than the owner of the data. If the data is confidential or personal, this can cause serious consequences for the application, the owner of the data, etc. You should consider what consequences result from this unauthorized disclosure.
- *Modify* transactions allow the modification of existing data. Unauthorized use can affect the integrity of the data and the ability to use the data for the purpose intended by the owner or other authorized users. Remember also that unauthorized modification of data also causes disclosure (i.e., the data is seen by an unauthorized user before they modify it). You should consider what consequences result when the integrity of the data is affected.
- *Delete* transactions allow data to be deleted temporarily or permanently. Unauthorized use causes the data to be unavailable to the owner and other authorized users. If the loss of data is temporary, you should consider what consequences result from having to recover or restore this data, and the inability to use it temporarily for the purposes intended. If the loss is permanent, you should consider what consequences result from the permanent inability to use this data for the purposes intended.
- *Create* transactions permit data to be recorded or documented. Unauthorized use can result in the creation of data that is misleading, fraudulent, or used for unintended purposes; essentially the integrity of existing data is put in question. The creation of unauthorized data can interfere with the use of existing data for authorized purposes. As with the unauthorized modification of data, you should consider what consequences result from the inability to use existing data for the purposes intended, or the use of data that may not be accurate.

### 9.6.3 Developing Consequence Statements

As you develop consequence statements, you need to consider the effects of unauthorized use as noted above. In addition, you should consider the consequence questions. These questions have been developed for each transaction type and prompt you to consider consequences as they relate to the various impact categories. (You were introduced to these areas when you reviewed the OMB impact criteria.) Thus, you develop consequence statements that reflect undesired outcomes and the effects on the application in areas such as reputation, financial loss, and personal safety.

### 9.6.4 Example of Consequence Statements

Composing effective consequence statements takes practice. Here is an example to guide your development of consequence statements: Consider a transaction that allows a user to inquire on a personal profile that they established to determine their eligibility for benefits. This profile contains significant personal data such as the user’s social security number and any health conditions that they currently have, such as diabetes.

If an unauthorized user performs this transaction, the undesired outcome is a disclosure of private information to other than the owner of the information or their authorized agent. What are the resulting consequences of this unauthorized use?

To determine these consequences, we look to the consequence questions for transaction type “inquire.” Consider the first question: What is the impact on the reputation of the application? This would result in the following consequence statement:

> *“The reputation of the application would be adversely affected. Users would not have confidence that we are adequately protecting users’ personal data, and therefore they would stop using the web site. This would destroy our mission to bring government to the people.”*

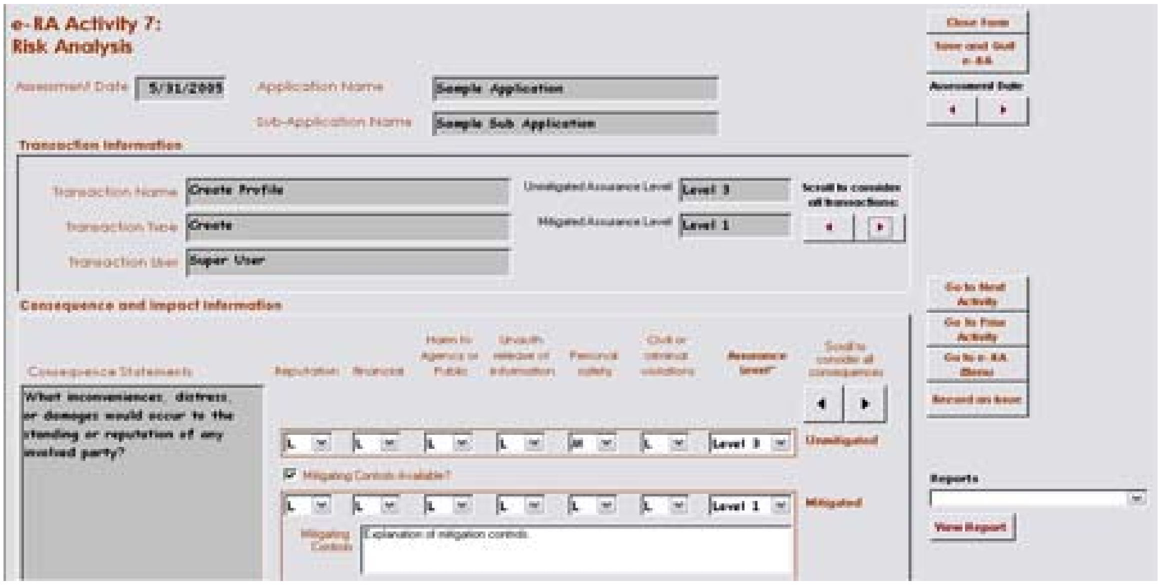
Consider another question: What fines and regulatory issues would we be exposed to? By answering this question, another consequence statement is generated:

> *“Disclosing a user’s private information would put the application in violation of the Privacy Act of 1963, and worse yet, would cause us to be out of compliance with HIPAA regulations. We would be fined $1,000, and probably be subjected to a Congressional Review or GAO audit.”*

Each of these consequence statements will play an important part in determining the appropriate level of authentication for transactions.

# 10 e-RA Risk Analysis

Provided below is the e-RA screen used to complete Activity 7 – Risk Analysis.



Assessment Date 5/31/2005

Application Name Sample Application

Sub-Application Name Sample Sub Application

Transaction Information

Transaction Name Create Profile

Transaction Type Create

Transaction User Super User

Unmitigated Assurance Level Level 3

Mitigated Assurance Level Level 1

Consequence and Impact Information

Consequence Statements

What inconveniences, distress, or damages would occur to the standing or reputation of any involved party?

| | Reputation | Financial | Harm to Agency or Public | Unauth. release of information | Personal safety | Civil or criminal violations | Assurance level* |
|---|---|---|---|---|---|---|---|
| Unmitigated | L | L | L | L | M | L | Level 3 |
| Mitigated | L | L | L | L | L | L | Level 1 |

☑ Mitigating Controls Available?

Mitigating Controls: Explanation of mitigation controls.

**Figure 9: Activity 7 – Risk Analysis**

## 10.1 Purpose

The purpose of this activity is to analyze the consequences of unauthorized use of transactions using the risk tolerance criteria for your application.

## 10.2 Background

Areas vital to achieving the organization's goals, objectives, and mission--such as reputation, customer confidence, finance, legal or regulatory, etc.--can be used to evaluate the consequences of unauthorized use.

When the consequences of unauthorized use are realized by the organization, these areas can be used to estimate the extent of the potential impact.

## 10.3 Important Tips

Always check the top portion of any form you are working in to see that you are on the correct assessment by date.

You may want to print the OMB Impact Criteria Report or your qualified criteria to aid you in performing this activity. The OMB Impact Criteria Report is available on the reports drop-down box and from the e-RA menu; use the item labeled View or Print e-RA reports.

## 10.4 Performing the Activity

Use the following steps to complete Activity 7 – Risk Analysis:

### 10.4.1 Part 1 – Impact Analysis

1. Check the shaded boxes at the top of the form to ensure that the date and name of the application (and sub-application, if applicable) is correct.
2. Check the Transaction Name, Transaction Type, and Transaction User boxes to confirm that you are assessing the intended transaction.

3. Review each consequence statement and consider the extent of impact on the organization if this consequence is realized. Refer to the OMB Impact Criteria to choose a value for the impact. Record this by selecting "high, medium, low, or N/A" values for each of the six impact categories for each consequence. (Understanding the OMB criteria will aid you greatly in this effort. In addition, remember to use your qualifications if you have developed them. This will give you greater insight into the extent of the impact.) For any impact category that you feel is not affected by the stated consequence, record the value as "N/A."

4. If there are mitigating controls available for the consequence statement, check the "Mitigating Controls Available?" checkbox. In light of the mitigating controls, review the consequence statement again, recording the mitigated impact in the six impact categories. Add an explanation of the mitigating controls in the box marked "Mitigating Controls."

5. Continue this activity for each consequence statement for a single transaction.

### 10.4.2 Part 2 – Choosing an Assurance Level

6. Select an appropriate unmitigated assurance level for each consequence and set of impacts. Choose the level that would be most effective in preventing the consequence and the resulting impacts from occurring. OMB provides standard definitions of the assurance levels in the e-Authentication Guidance for Federal Agencies. To view these definitions, click on the "OMB Auth Level Definitions" button. In addition, as an aid in determining which levels are appropriate for preventing a particular consequence from resulting in an impact in the six impact categories, OMB has provided a matrix which relates impact categories to levels. This matrix is available by clicking on the "OMB Impact/Level Matrix" button.

7. If mitigating controls are available, select an appropriate mitigated assurance level.

8. Click on the arrow buttons next to "Scroll to consider all transactions" to advance to the next transaction or move to prior transactions to revise.

9. Repeat steps 2-6 until you have selected impact values and an authentication level for each consequence of all transactions. **Note: It is important that you assign an authentication level to each consequence statement for each transaction. These levels will guide you in the next activity to decide upon an overall level for the transaction.**

10. Click on the "Go to Next Activity" button

## *10.5 Other Issues*

At any time, you may click the button labeled "Record an Issue" to go to a form for capturing issues and concerns that arise during the assessment.

## *10.6 Concepts*

### 10.6.1 Impact of Unauthorized Use

Even though consequences may result from unauthorized use of transactions, there may be no appreciable impact on the application. For example, if an unauthorized user inquires on public data or information, a consequence could be that the agency is embarrassed because of a breach in security, but if that is only known internally to a few trusted insiders, there may be minimal overall impact on the application. However, if this becomes front page news in the *Washington Post*, the impact is much greater.

You reviewed and qualified the OMB impact criteria in Activity 3 so that you can measure the impact of consequences of unauthorized use of transactions specific to your application. If appearing on the front page of the *Washington Post* in a negative way is a particularly undesirable outcome for your application, you may consider this impact to be “high” based on your risk-tolerance criteria.

By determining the impact of a consequence, you are fully documenting the risk of unauthorized use of transactions for the application. Thus, risk is fully defined as the threat of unauthorized use, the consequences of realizing this threat, and the impact or extent to which the application is affected by these consequences.

### 10.6.2 Origin of Assurance Levels

For simplicity and consistency, assurance levels are used in e-RA to describe the various degrees of proving the identity of users. The developers of the e-RA approach have included the assurance levels that are recommended by OMB. Theoretically, users of e-RA could substitute any assurance schema that works for them. The basic e-RA process is flexible and can be matched with a variety of assurance levels.

Remember: If you are using the e-RA approach and are bound by OMB guidelines, you should adhere to OMB’s definitions of assurance levels as you perform your assessment. For convenience, the definition of assurance levels as provided in OMB’s “e-Authentication Guidance for Federal Agencies” is provided in Appendix C of this document.

### 10.6.3 Purpose of Assurance Levels

In e-RA, the assurance levels have two primary purposes:

- to define the characteristics of authentication that a transaction would need to deploy to prevent risks of unauthorized use from being realized
- to provide a foundation for the development of detailed assurance requirements for a transaction that can be translated into technical requirements for implementation

It is important to note that the levels do not represent any particular assurance requirements or technical solutions.

In e-RA, the assurance levels are assigned first to the risks of unauthorized use for each transaction. Then, based on these assurance levels, an overall assurance level is assigned to the transaction. These transaction level assurance levels are then used to create an overall assurance level for each user role.

### 10.6.4 Selecting Assurance Levels for Each Risk

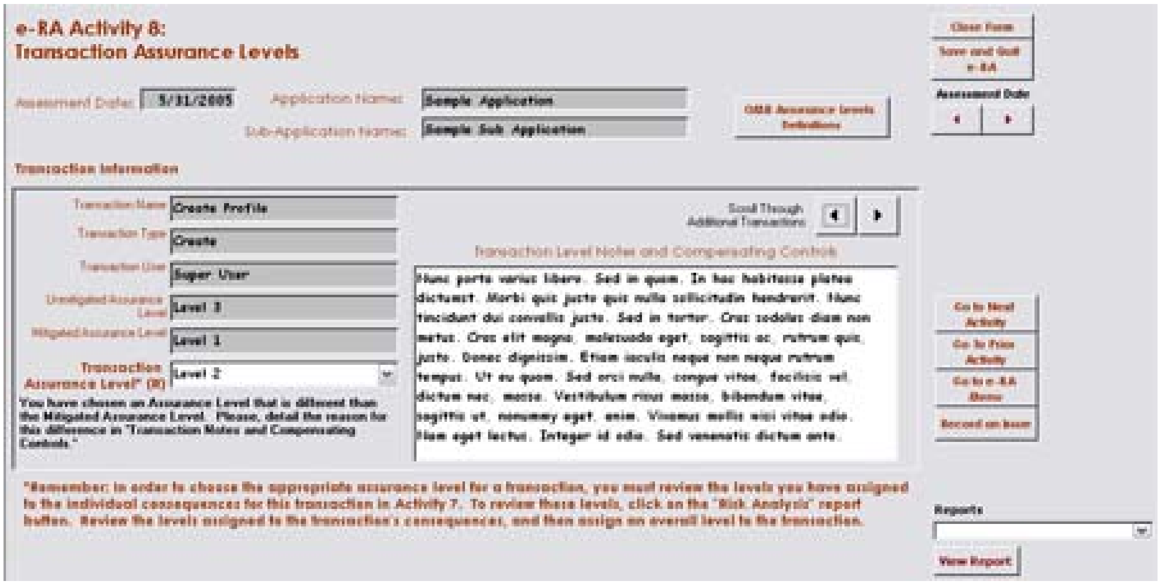
The identification of risks provides further information regarding the extent to which the organization must develop and implement corresponding preventive controls (such as authentication) to mitigate the overall risk.

The first step in determining these authentication controls for a transaction is to determine the appropriate assurance levels for each risk that you have identified for each transaction. Thus, you should assign an assurance level for each risk (i.e., consequence statement and impacts) that you identified. These levels will help you in the next activity to determine an overall assurance level for a transaction.

To assign a level for each risk, you review each consequence statement and the impact values (that you have assigned to this statement) in each of the six impact categories. This information is used to determine the assurance level that would prevent this consequence and resulting impacts from occurring. **You perform this for every consequence that you have identified for a transaction.**

# 11 e-RA Transaction Assurance Levels

Provided below is the e-RA screen used to complete Activity 8 – Transaction Assurance Levels.



e-RA Activity 8:
Transaction Assurance Levels

Assessment Date: 5/31/2005
Application Name: Sample Application
Sub-Application Name: Sample Sub Application

Transaction Information

Transaction Name: Create Profile
Transaction Type: Create
Transaction User: Super User
Unmitigated Assurance Level: Level 3
Mitigated Assurance Level: Level 1
Transaction Assurance Level* (R): Level 2

You have chosen an Assurance Level that is different than the Mitigated Assurance Level. Please, detail the reason for this difference in "Transaction Notes and Compensating Controls."

Transaction Level Notes and Compensating Controls:
Nunc porta varius libero. Sed in quam. In hac habitasse platea dictumst. Morbi quis justo quis nulla sollicitudin hendrerit. Nunc tincidunt dui convallis justo. Sed in tortor. Cras sodales diam non metus. Cras elit magna, malesuada eget, sagittis ac, rutrum quis, justo. Donec dignissim. Etiam iaculis neque non neque rutrum tempus. Ut eu quam. Sed orci nulla, congue vitae, facilisis vel, dictum nec, massa. Vestibulum risus massa, bibendum vitae, sagittis ut, nonummy eget, enim. Vivamus mollis nisi vitae odio. Nam eget lectus. Integer id odio. Sed venenatis dictum ante.

*Remember: in order to choose the appropriate assurance level for a transaction, you must review the levels you have assigned to the individual consequences for this transaction in Activity 7. To review these levels, click on the "Risk Analysis" report button. Review the levels assigned to the transaction's consequences, and then assign an overall level to the transaction.

**Figure 10: Activity 8 – Transaction Assurance Levels**

## 11.1 Purpose

The purpose of this activity is to assign an assurance level to each transaction.

## 11.2 Background

At the transaction level, all of the risks (consequences of unauthorized use and their impact values) and their corresponding assurance levels must be considered to derive an assurance level for the transaction. There is no automatic process for doing this. It is a reasoning activity that requires the participants' knowledge and experience.

## 11.3 Important Tips

Always check the top portion of any form that you are working in to see that you are on the correct assessment by date.

You may want to print the Transaction Summary Report to aid you in performing this activity. The report is available from the reports drop-down box and from the e-RA menu.

## 11.4 Performing the Activity

Use the following steps to complete Activity 8 – Transaction Assurance Levels:

1. Check the shaded boxes at the top of the form to ensure that the date and name of the application (and sub-application, if applicable) is correct.

2. Review the assurance levels that you assigned to each of the risks (consequences and impacts) for each transaction.

3. Select an assurance level for the transaction.

4. Record any notes relevant to your selection. If you have chosen an assurance level that is different from the (provided) highest existing assurance level associated with the transaction's risks, you must provide an explanation.

   For example, if you have assigned a "level two" to most of the transaction risks, but you have one "level three," you may still decide to assign "level three" to the overall transaction. You may record a note that indicates that the single "level three" risk is particularly undesirable and would need to be avoided, and therefore it is driving the overall transaction assurance level.

5. Repeat this process for all transactions.

6. Click on the "Go to Next Activity" button.

## *11.5 Other Issues*

At any time, you may click the button labeled "Record an Issue" to go to a form for capturing issues and concerns that arise during the assessment.

## *11.6 Concepts*

### 11.6.1 Selecting Assurance Levels for Each Transaction

The penultimate step in performing an e-RA assessment is to determine the assurance level that, based on risk, should be assigned to a transaction. There is no automatic means for doing this; it is an activity that requires the reasoning and knowledge of the application participants who are performing the assessment.

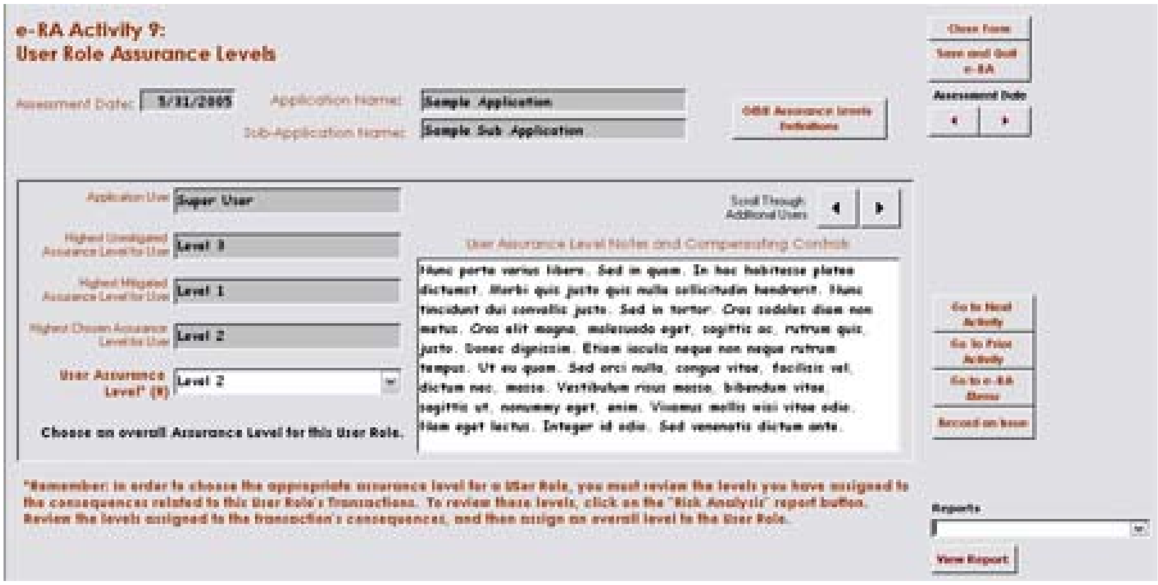
The basis for determining the transaction assurance level is the assurance levels you assigned to each transaction risk (consequence and impacts). You must look across these levels and resolve an overall level that is representative of all risks for the transaction. In some cases, this is simple—the assurance levels for each risk are the same, and therefore the transaction assurance level is the same. However, most often, you will have many different assurance levels assigned to individual risks for a transaction. To select an appropriate assurance level for a transaction, you must look at these levels and consider the risks to which they have been assigned. For example, consider that you have 10 risks identified for a transaction, and you have assigned assurance levels as follows:

- two risks were assigned "level 1"
- three risks were assigned "level 2"
- four risks were assigned "level 3"
- one risk was assigned "level 4"

In this case, you might assume that the overall transaction should be assigned a "level 4." However, this may be cost prohibitive and you may decide that the majority of risks that you want to avoid are at "level 3." As a result, you assign a "level 3" to the transaction and decide to implement other types of controls to mitigate the one risk that required a "level 4." This is perfectly acceptable because you are making a risk-based decision, rather than a purely technical decision, which is in keeping with the underlying philosophy of the e-RA approach.

# 12 e-RA User Role Assurance Levels

Provided below is the e-RA screen used to complete Activity 9 – User Role Assurance Levels.



e-RA Activity 9:
User Role Assurance Levels

Assessment Date: 5/31/2005

Application Name: Sample Application

Sub-Application Name: Sample Sub Application

Application User: Super User

Highest Unmitigated Assurance Level for User: Level 3

Highest Mitigated Assurance Level for User: Level 1

Highest Chosen Assurance Level for User: Level 2

User Assurance Level* (8): Level 2

Choose an overall Assurance Level for this User Role.

User Assurance Level Notes and Compensating Controls

Nunc porta varius libero. Sed in quam. In hac habitasse platea dictumst. Morbi quis justo quis nulla sollicitudin hendrerit. Nunc tincidunt dui convallis justo. Sed in tortor. Cras sodales diam non metus. Cras elit magna, malesuada eget, sagittis ac, rutrum quis, justo. Donec dignissim. Etiam iaculis neque non neque rutrum tempus. Ut eu quam. Sed orci nulla, congue vitae, facilisis vel, dictum nec, massa. Vestibulum risus massa, bibendum vitae, sagittis ut, nonummy eget, anim. Vivamus mollis nisi vitae odio. Nam eget lectus. Integer id odio. Sed venenatis dictum ante.

*Remember: in order to choose the appropriate assurance level for a User Role, you must review the levels you have assigned to the consequences related to this User Role's Transactions. To review these levels, click on the "Risk Analysis" report button. Review the levels assigned to the transaction's consequences, and then assign an overall level to the User Role.

**Figure 11: Activity 9 – User Role Assurance Levels**

## 12.1 Purpose

The purpose of this activity is to assign an assurance level to each user role.

## 12.2 Background

At the user role level, all of the transactions and their corresponding assurance levels must be considered to derive an assurance level for the user role. There is no automatic process for doing this. It is a reasoning activity that requires the participants' knowledge and experience.

## 12.3 Important Tips

Always check the top portion of any form that you are working in to see that you are on the correct assessment by date.

## 12.4 Performing the Activity

Use the following steps to complete Activity 9 – User Role Assurance Levels:

1. Check the shaded boxes at the top of the form to ensure that the date and name of the application (and sub-application, if applicable) is correct.

2. Review the assurance levels that you assigned to each of the transactions.

3. Select an assurance level for the user role.

4. Record any notes relevant to your selection. If you have chosen an assurance level that is different from the (provided) highest existing assurance level associated with the transaction's risks, you must provide an explanation.

5. Repeat this process for all user roles.

6. Click on the "Go to Next Activity" button.

## *12.5 Other Issues*

At any time, you may click the button labeled "Record an Issue" to go to a form for capturing issues and concerns that arise during the assessment.

## *12.6 Concepts*

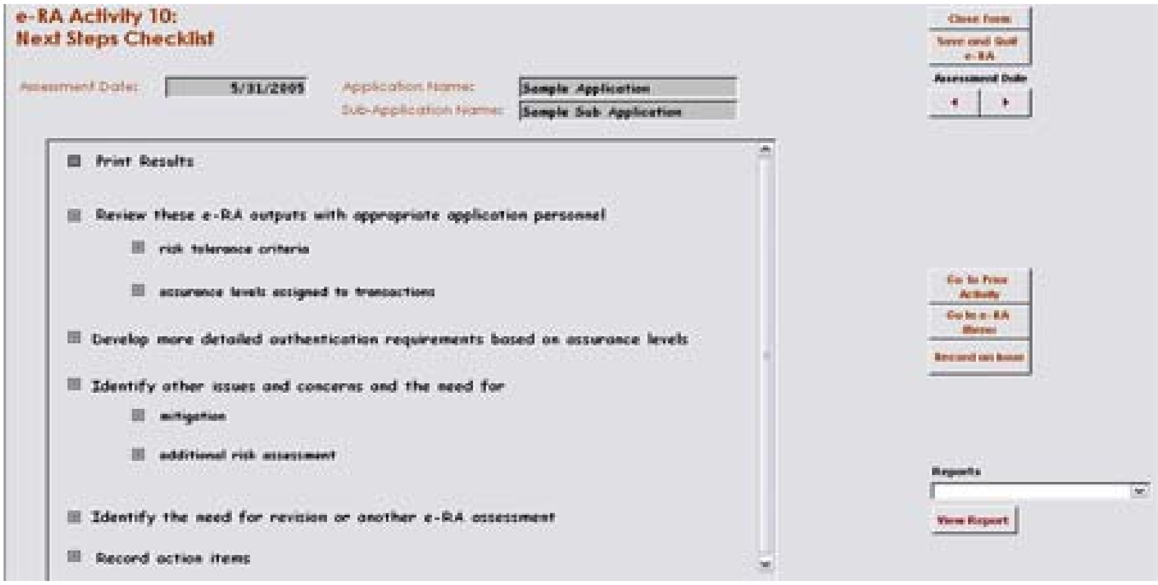
### 12.6.1 Selecting Authentication Levels for Each Transaction

The final step in performing an e-RA assessment is to determine the assurance level that, based on the risk associated with all transactions, should be assigned to a user role. There is no automatic means for doing this; it is an activity that requires the reasoning and knowledge of the application participants who are performing the assessment.

The basis for determining the user role assurance level is the assurance levels you assigned to each transaction. You must look across these levels and resolve an overall level that is representative of all transactions. In some cases, this is simple—the assurance levels for each transaction are the same, and therefore the user role assurance level is the same. However, most often, you will have many different assurance levels assigned to individual transactions. To select an appropriate assurance level for a user role, you must look at these levels and consider the transactions to which they have been assigned.

# 13 e-RA Next Steps

Provided below is the e-RA screen used to complete Activity 10 – Next Steps Checklist.



e-RA Activity 10:
Next Steps Checklist

Assessment Date: 5/31/2005
Application Name: Sample Application
Sub-Application Name: Sample Sub Application

- ▪ Print Results
- ▪ Review these e-RA outputs with appropriate application personnel
  - ▪ risk tolerance criteria
  - ▪ assurance levels assigned to transactions
- ▪ Develop more detailed authentication requirements based on assurance levels
- ▪ Identify other issues and concerns and the need for
  - ▪ mitigation
  - ▪ additional risk assessment
- ▪ Identify the need for revision or another e-RA assessment
- ▪ Record action items

**Figure 12: Activity 10 – Next Steps Checklist**

## 13.1 Background

You have completed e-RA. This form is provided as a convenience to help you with next steps.

## 13.2 Performing the Activity

Use the following steps to complete Activity 10 – Next Steps Checklist:

1. Review the checklist for possible actions.

2. Review and discuss anything you recorded in the Issues form.

3. Take action or record who will do the action and by what date.

4. Click on the button labeled “Go to e-RA Menu” to continue working on assessments or click on “Quit e-RA” to stop work.

## 13.3 More Information

You may want to review the information developed, documented, and analyzed in the e-RA approach with other staff in the application (or other stakeholders) to ensure their understanding and agreement. This includes:

- the impact criteria and qualifications used
- e-RA outputs, including the documentation of transactions, consequences, and their impact values
- the mapping of risks and transactions to assurance levels
- the other issues and concerns documented throughout the e-RA assessment

The value of discussing this information with the various stakeholders for the application is high. In these conversations, more information about the authentication needs of the application may be developed and considered. Important note: If you make changes to the risk-tolerance criteria based on these conversations, this can affect the analysis you performed in the process. You may need to go back and re-value the impacts of consequences. This might ultimately affect the mapping of risks and transactions to the assurance levels.

Remember that the assurance levels chosen for transactions may not entirely prevent the individual risks that you identified. In some cases, you will need to identify additional mitigation actions that are necessary (in addition to the assurance levels assigned to the transaction) to ensure proper preventive controls.

In addition, you may want to document detailed authentication requirements that are representative of the types of preventive controls that are necessary to ensure proper authentication. The assurance levels you assigned to transactions and user roles are a component of these requirements, but do not completely define the requirements.

Finally, the other issues and concerns identified throughout the e-RA activities need to be addressed. You may want to discuss these concerns with appropriate staff in the organization to determine if your concerns are legitimate, and whether any actions have been taken to mitigate them. You should develop mitigation strategies for those issues and concerns that you feel are not being addressed. You might also want to use this information as the basis for performing a more detailed risk assessment that covers the areas of risk to which an E-Government application may be exposed.

# 14 Importing and Exporting Data with e-RA

## 14.1 Exporting Data into Excel Spreadsheets

Oftentimes, users will have a need to get their data in a more controllable format. In these situations, it is recommended that they export their e-RA information into a Microsoft Excel spreadsheet. Users should perform the following steps in order to export their data:

1. Open the e-RA database/tool that currently contains the data you wish to export.
2. Accept the e-RA warranty.
3. Close the “Main Menu” window by clicking on the red x in the upper right corner of the “Main Menu” window.
4. You will now find yourself with one window open; this window will be titled something to the effect of “eRA 1.5 : Database (Access 2002 – 2003 file format)” (exact wording will vary based on the file format you are using). In this window, click on the “Tables” option on the menu on the left side of the window.
5. Ignoring the first three options (“Create Table in Design View”, “Create Table by using wizard”, and “Create Table by entering data”), click on each of the tables and perform the following steps:
   a. Go to the “File” menu and choose “Export.”
   b. This brings up a Microsoft Windows “Save” style window, titled “Export Table “XYZ” To …” where XYZ is the table you have selected.
   c. Change the “Save As Type” to “Microsoft Excel 97-2003 (*.xls)”
   d. Enter a meaningful name in the “File Name” box.
   e. Click on the “Export” button.
   f. Repeat for all tables
6. Once completed, close e-RA.

## 14.2 Importing Data from one e-RA Database to Another

The e-RA tool is designed to be a stand-alone tool, not working in a networked environment; it is highly recommended that the tool be used in this fashion. Because of this stand-alone design, importing data from one e-RA database to another e-RA database carries some inherent risks. Due to certain database design features (in this case, “Primary Keys” and “Foreign Keys,” structures used to tie disparate data together) the opportunity for data corruption is high. In short, in the likely event that the two stand-alone databases have the same keys, the resulting database will not work as expected.

## 14.3 Importing Data from e-RA v1.4b to e-RA v1.5

Considering the stand-alone design, importing data from an e-RA v1.4b database to an e-RA v1.5 database carries some inherent risks. In addition to the technical risks discussed in the preceding section, there are functional reasons to not import from v1.4b to v1.5. e-RA v1.5 contains two major new pieces of functionality: user roles and mitigation. This information is required in the new tool and not available in older versions of the tool. If you have previously gone through the e-RA process and are moving to a new version of the tool, it is recommended that you manually copy information from the old tool to the new tool, performing the required user role and mitigation analysis as you go.

# Appendix A: Glossary

| | |
|---|---|
| **Authentication** | One technique for identity management and access control; a way to ensure that users are who they say they are—that the user who attempts to perform functions in a system is in fact the user who is authorized to do so. |
| **Assurance Levels** | The assurance levels depict various aspects of user identity and authentication that a transaction might need to deploy. The levels are used in deciding the appropriate level of assurance necessary to mitigate or prevent risks identified during the e-RA approach. Developers of e-RA used the levels of assurance roughly based on the UK standards and consistent with forthcoming OMB standards. However, users of e-RA could substitute any authentication schema that works for them. The basic e-RA process is flexible and can be matched with a variety of assurance levels. |
| **Assurance Levels** | The characteristics of authentication that a transaction would need to prevent risks of unauthorized use from being realized. The foundation for the development of detailed authentication requirements for a transaction that can be translated into technical requirements for implementation. |
| **Authentication Risk** | Risk that could be avoided by appropriate authentication. The risks to which the application, its users, and its business partners would be subjected if unauthorized use of transactions occurs. |
| **Common Transactions** | Transactions that are used most frequently. |
| **Consequence Statement** | A description of the effects of unauthorized use of a transaction. |
| **Critical Transactions** | Transactions most relevant to the purpose or mission, or without which the application could not fulfill its primary objectives. |
| **Delete transaction** | A transaction that allows the user to destroy or eliminate data or information so that it is no longer available for inquiry or modification. The elimination of data or information may be temporary (recoverable) or permanent (unrecoverable). |
| **e-RA** | The e-Authentication Risk and Requirements Assessment approach. It is a risk-based technique to elicit authentication requirements for transactions. |
| **Impact** | The effect on the organization of a risk being realized; the effect of one thing on another. |
| **Impact Area or Category** | Impacts categorized or arranged by the type of impact that they describe and used to measure the extent of the effect on the organization. Impact areas are reputation, financial loss, harm to agency programs, unauthorized release of sensitive information, personal safety, and civil or criminal violations. |

| | |
|---|---|
| **Inquire Transaction** | A transaction that allows the user to access data or information. The user makes a request for information and receives it. This information may be related to the user in some way (i.e., private) or can be general information (i.e., public.). |
| **Modify Transaction** | A transaction that allows the user to modify existing data or information in a system and save those changes. The original information may or may not be recoverable. |
| **Non-repudiation** | Specific identification of a user plus the need to specifically link the user to a transaction; i.e., to prove that the user intended to be bound by the transaction. |
| **Range of Transactions** | A set that represents all the types of transactions. The upper and lower limits of the transactions in terms of what they allow users to do. |
| **Risk-based Approach** | The requirements elicited using e-RA are representative of, and derived from, the types of risks that the organization is trying to avoid. |
| **Risk-tolerance Criteria (Impact Criteria)** | These criteria are benchmarks or measures against which the organization can evaluate the impacts of unauthorized use of an application's transactions. |
| **Security Requirements** | Security requirements are the foundation of information security. They are: confidentiality, integrity, and availability. Authentication and non-repudiation are sometimes also characterized as security requirements. Security requirements embody many of the concepts important to the authentication process. Violations of security requirements as the result of unauthorized use of transactions and the resulting undesired outcomes directly affect the organization and are reflected in the types of impacts that can be identified. |
| **Transaction** | The transactions of a system are the specific actions that users can perform to achieve a desirable result. A transaction is an actor, plus an action, resulting in a desired outcome. |
| **Transaction Data** | Transactions are the vehicle for creating system data, inquiring on it, modifying it, or deleting it. Authentication is one control used to ensure that data, both personal and organizational, is protected from unauthorized actions. Considering the value of data accessed by transactions helps e-RA users to realize the consequences of unauthorized use and choose appropriate assurance levels. |
| **Transaction Levels** | The assurance level for a transaction, considering all of the risks (consequences of unauthorized use and their impact values) and their corresponding assurance levels. |
| **Transaction Types** | Four types of transactions for web-based systems: create, delete, inquire, and modify. |
| **Unique Transactions** | Transactions that are neither common nor ordinary and that may have a special purpose or distinctive users. |

| | |
|---|---|
| **User Role** | Definitions of user types who interact with the application by enacting transactions.  Examples include administrators, approvers, users and super users. |
| **User Role Levels** | The assurance level for a user role, considering all of the transactions and their corresponding assurance levels. |

# Appendix B: Using Forms

There are ten basic activity forms in the e-RA tool:

Activity 1: Application Description – record the basic information about an application

Activity 2: Assessment Information – document the assessment date and the participants who performed the assessment

Activity 3: Risk Tolerance Criteria – identify the tolerance for risk in your specific organization

Activity 4: User Roles – identify the user roles associated with the application's users

Activity 5: Transaction Identification – identify transactions that an application offers

Activity 6: Risk Identification – identify the consequences of unauthorized use of the transactions

Activity 7: Risk Analysis – apply the risk-tolerance criteria to the consequences of unauthorized use of transactions

Activity 8: Transaction Assurance Levels – assign assurance levels to each transaction

Activity 9: User Role Assurance Levels – assign assurance levels to each user role

Activity 10: Next Steps – use checklist to reflect completion of the e-RA process and post-assessment activities

## *1.1 Form Components*

e-RA activity forms are composed of labels, fields, and buttons. Labels are made up of text that identifies specific information related to the form, such as sections or fields. The boxes, or fields, display the data stored in the tool. Different fonts are used in the forms to differentiate between labels and data entered and stored in the tool. Buttons allow you to navigate and perform actions in the form and entire tool.

The forms are generally presented in zones. Each form has:

- a title in the upper left-hand corner
- a body consisting of all of the fields
- buttons along the right side

Each of these form characteristics are shown below in Figure 13.

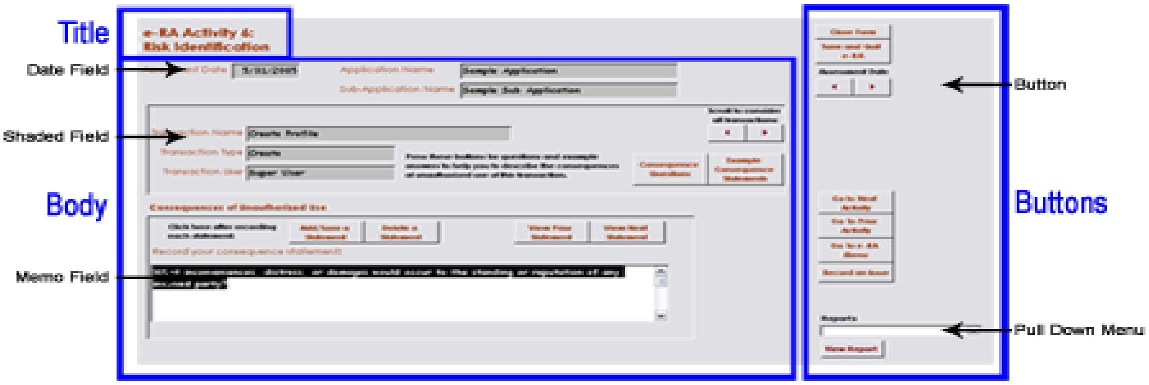


Figure 13: e-RA Form Example

## *1.2 Form Fields*

### 1.2.1 Shaded Fields

Many forms display shaded fields. The data displayed in these fields has already been entered in previous forms. Data in shaded fields cannot be changed unless you change it where it originates. For example, you cannot change an assessment date unless you do so in the Assessment Information form.

Shaded fields frequently include data about the application and the assessment date.

⚠ **You should refer to these fields frequently to ensure that you are working on the correct assessment.**

### 1.2.2 White Fields

White fields are used for data entry. They can capture data in several different formats. Those fields marked with an “(R)” are required. You must enter data into these fields to proceed. Types of data-entry fields include date fields, text boxes, check boxes, and pull-down menu boxes. Each of these data entry fields are explained below:

- *Text boxes* allow free-form entry of data. There are no formatting restrictions. Whenever you exceed the visible space of the text box, a scroll bar will appear.
- *Date fields* accept a date in the format of a two-digit month and day, and a four-digit year (mm/dd/yyyy). As you type into this field, your data will automatically be formatted as noted.
- *Check boxes* are small white boxes with text in line next to them. You may select as many choices as are available on the form. A box appears as checked when you click in the white space of the box.
- *Pull-down menus* look like a text box, but have a button with a picture of an arrow on it in the right side of the box. When you click on this arrow, a menu appears with a number of choices. Select the appropriate choice by dragging your mouse down the list and clicking on your selection.

### 1.2.3 Buttons

Buttons are generally displayed along the right side of a form. They are divided into sections that are labeled with their actions. Buttons allow you to navigate and perform certain actions in the form and in the entire tool.

## *1.3 Form Navigation*

You may navigate the e-RA forms by using your mouse, <Tab> key, <Enter> key or arrow keys.

### 1.3.1 Tab Order

Tab order on the e-RA forms has been predefined based on ease of data entry. Upon opening a form, the cursor will be positioned in the first available field where you are able to enter data. When you have completed a field, you can move to the next field by doing one of the following:

- pressing the <Tab> key or
- positioning your mouse to click in the next box or
- pressing the <Enter> key

You cannot tab through check box lists and buttons. To access these boxes and buttons, you must position your mouse on them. If you tab through all of the white fields on a form, you will advance to a new clean form.

⚠ **Be cautious — don't advance through the white fields until you have entered data in the check boxes. Otherwise, you will have to go back and edit the previous form.**

### 1.3.2 Buttons

Each type of button is shown below in Figure 14.

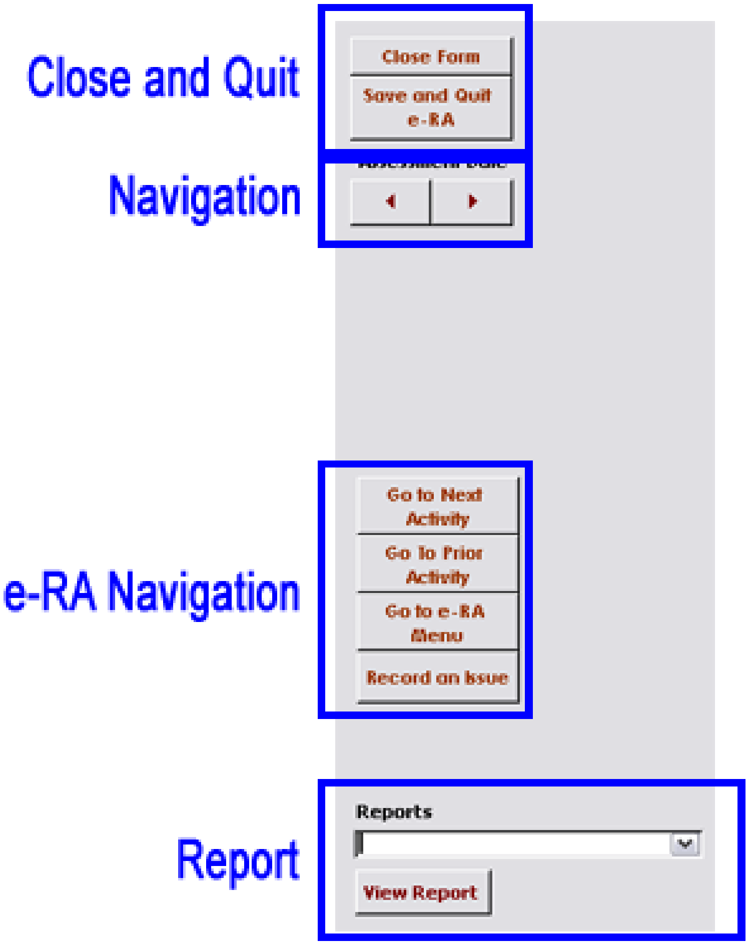


**Figure 14: e-RA Buttons Example**

Form buttons are clustered and positioned close to the data that they pertain to. They perform the following actions:

- open a form
- close a form
- quit the tool
- add or save data
- delete data
- move to the prior record in the database
- move to the next record in the database
- open a report
- go to the e-RA Menu

### 1.3.3 Close and Quit

The buttons in the upper right-hand corner of every form will close the form or quit the e-RA tool.

⚠ **Caution: If you quit the e-RA tool, there is a chance that the data you have entered on the form will not be saved. You must click "Add/Save" before you choose "Quit e-RA" on forms where an Add/Save button appears.**

### 1.3.4 Function Buttons

Function buttons relate to the core of the data that is being entered for a specific e-RA activity. For example, if you are entering data into the Transactions form, the function buttons indicate example transactions, add/delete a transaction, and view next and prior transactions.

On each form where these buttons appear, they perform the same basic functions:

- Add/Save – this is a dual-purpose button. When pressed, it will save the data you have entered and advance to a blank form. It is suggested that you save often. However, note that if you add/save before you have completed the entire form, you will need to return to the form later to complete the remaining fields.
- Delete – this button will not only delete the information entered in the form where the cursor is located, but all information related to that data. For example, if you delete an assessment date, all e-RA information associated with that date will also be deleted. You will receive a warning when you initiate this action, when a warning is applicable.
- Prior and Next – these buttons allow you to move back and forth between data that you have entered.

### 1.3.5 Assessment Navigation

The assessment date is the primary identifier for storing information in the e-RA tool and affects navigation. As you enter data on the forms, you must check the top of the form to ensure that you are working on the correct assessment. Navigation buttons have arrows on them.

The assessment navigation buttons allow you to move back and forth among all of the assessments that you have performed. If you only have one assessment, these buttons are moot. However, if you would like to review data from a previous assessment, use the button with the red arrow pointing to the left to go back to a previous assessment and then the button with the red arrow pointing to the right to return to the current assessment.

### 1.3.6 e-RA Navigation

The e-RA navigation buttons allow you to go to other areas of the tool. They perform the following functions:

- "Record an Issue" – opens the "Issues and Concerns" form.
- "Go to Prior Activity" – opens the previous activity form in the e-RA assessment and closes the current form.
- "Go to Next Activity" – opens the next activity form in the e-RA assessment and closes the current form.
- "Go to e-RA Menu" – takes you to the e-RA menu and closes the current form.

### 1.3.7 Other Buttons

There are also a few unique buttons that appear on some forms. Some of these buttons uniquely describe the action that will occur upon a click. Common actions of these unique buttons are:

- add the current record
- delete the current record
- view the prior records entered in the database
- view the next records stored in the database

- provide examples – for example, a list of transaction statements from a button on the Transaction Identification form
- offer guidance – on the Risk Identification form, a button will open a list of questions that will aid in your determination of consequences of unauthorized use of a transaction; the list of questions varies according to the type of transaction that you are examining
- scroll through previously entered data

⚠ **Saving data in a form—no data is saved in a form until you have tabbed through all fields to a blank form, or pressed the “Add/Save” button.**

# Appendix C: Viewing Assessment Reports

Thirteen tool reports present the data collected in the e-RA process. These reports will allow you to distribute information and check your work. They are titled:

- Executive Summary
- Application Detail
- Application Information
- Application Risk-Tolerance Criteria
- Default Risk-Tolerance Criteria
- Transaction Summary
- Risk Identification
- Risk Analysis
- Transaction-Level Summary
- User Role-Level Summary
- Issues
- Next Steps
- Ad Hoc

## *1.1 Report Presentation*

Printing all of the reports will give you a complete picture of all of your application information or a specific assessment. Through reports, the e-RA tool gives you the opportunity to view all recorded data. From there, you may review, distribute, and check your information.

Each report summarizes information for each activity in the e-RA process. Reports will only display data that has been properly saved in the tool. You may generate reports by choosing a report from the e-RA Menu or from the report drop-down list on any form within the tool. When you click on a button to see a report, some reports display a box that prompts the user for an assessment date. The message in this box reads, "Enter an Assessment Date (OK for all Dates)." At this point, you have two options:

- Type in an assessment date to view data collected for a specific assessment. Use the format of a two-digit month and day, and a four-digit year (mm/dd/yyyy).
- Press the <Enter> key on your keyboard to view the data for all assessments.

If you've chosen the Ad Hoc report, you will be provided with a number of prompts. As with the assessment date boxes, enter information only if you want to limit the data returned in the report. The Ad Hoc report allows you to view information limited by:

- Application Name
- Assessment Date
- Participants
- User Role Assurance Level
- User Role
- Transaction Assurance Level

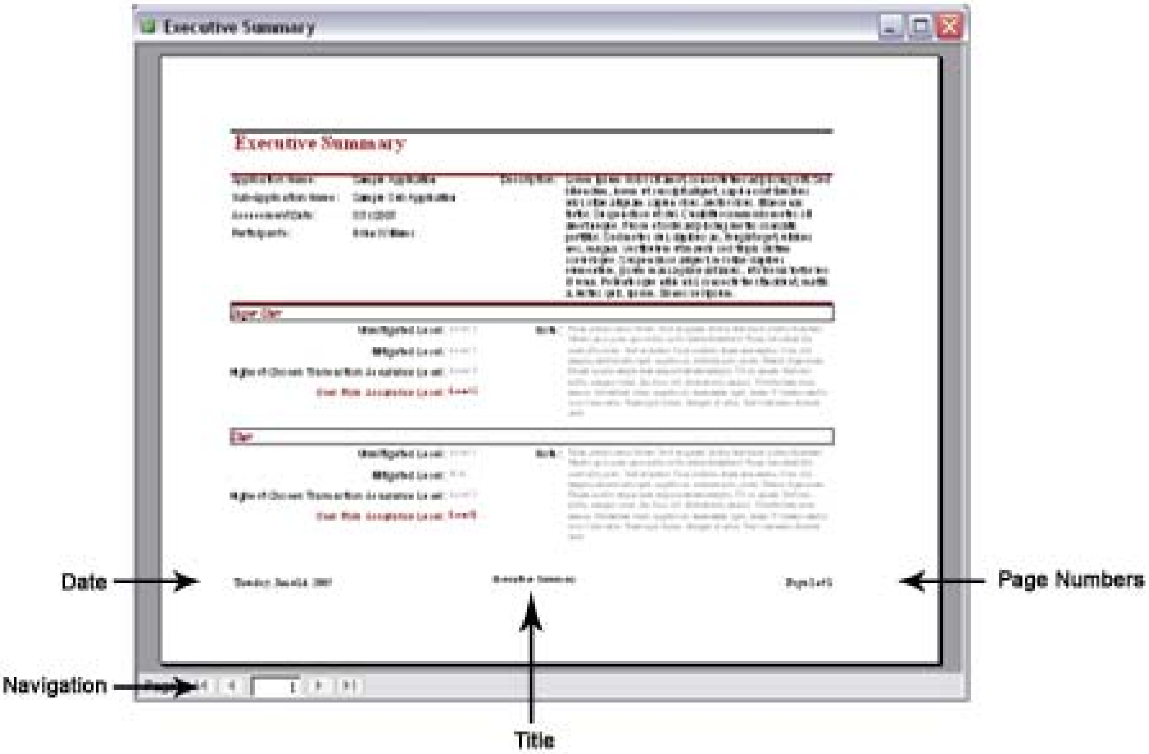


**Figure 15: Report Example**

Report features include the following:

- The date that the report is generated is in the lower left-hand corner.
- A page navigation button is below the date in the lower left-hand corner of the sheet.
- Page numbers and the number of pages are in the lower right-hand corner of the sheet.
- The report title will be displayed in the lower-center of the sheet.
- Reports will group and sort on specific data.

To close a report, click on the "X" in the upper right-hand corner of the box that the report is in.

⚠ **If the report is being viewed full-screen, you must minimize the report screen before closing it.**

Various reports have been illustrated below and outlined with specific information about each.

### 1.1.1 Application and Assessment Description

This report is used to report on both Activities 1 and 2 and displays the following information:

- Application Name
- Sub-Application Name
- Application Description
- Application Category
- Application Entry Points
- Application Assessment Date – listed with participants next to each date
- Participants – for each assessment date

### 1.1.2 Application Risk-Tolerance Criteria

This report shows the data recorded in Activity 3:

- Application Name – grouping the information below
- Sub-Application Name – along with the application name, form the overall heading and act as separator of the information
- Impact Areas – listed along the left-hand side of the report
- High, Medium, and Low criteria – decided by the organization performing e-RA for each impact area

### 1.1.3 Default Risk-Tolerance Criteria

You may use this report as a reference as you develop the Risk-Tolerance Criteria for your application in Activity 3. This report shows general high, medium, and low criteria for each impact area.

### 1.1.4 Transaction Summary

The Transaction Summary report provides information regarding all transactions for a particular assessment date. Use this report to show the data that you entered in Activity 5. This report will show the following information:

- Application Name
- Sub-Application Name
- Assessment Date
- Transaction Name
- Transaction Type
- Transaction Description
- Transaction Data
- Non-Repudiation – check box
- Other Information – recorded about the transaction
- Transaction Users

### 1.1.5 Risk Identification

This report lists the consequence statements for each transaction recorded in one assessment.

### 1.1.6 Consequence Questions

Use this report as a reference while completing Activity 6: Risk Identification. In this exercise, you describe the consequences of unauthorized use of a transaction by transaction type. This report will show the comprehensive list of questions for each type of transaction.

### 1.1.7 Risk Analysis

Use this report with Activity 7, in which you record the values for each consequence statement in an assessment. The following information will be on this report:

- Assessment Date
- Application Name
- Sub-Application Name
- Transaction Name
- Transaction Assurance Level – this item is added to the report after Activity 7
- Consequence Statements – for each transaction

- Impact Values in Reputation, Health, Productivity, Administrative, Regulatory, Finance, and Fines – these are lined up with the consequence statements on the report
- Consequence Assurance Level – for each consequence statement

### 1.1.8 Transaction Level Summary

This report lists the transactions for each assessment and their corresponding assurance levels. You choose these assurance levels in Activity 8.

### 1.1.9 User Role Level Summary

This report lists the user roles for each assessment and their corresponding assurance levels. You choose these assurance levels in Activity 9.

### 1.1.10 Next Steps Checklist

This report will capture any next steps in an assessment. It is in a checklist format as it is on the Activity 10 form.

### 1.1.11 Issues

This report has the list of issues that you recorded while going through the e-RA process. This report also shows the Issue Category and Mitigation that you documented for each issue.

### 1.1.12 Executive Summary

This report displays a high level overview of the application and its chosen user-role assurance levels. This report also shows the highest assurance levels related to each user-role's transactions and provides notes explaining discrepancies.

### 1.1.13 Application Detail

Similar to the Executive Summary report, this report displays an overview of the application and its chosen, user-role assurance levels. In addition, this report also provides information related to each individual transaction and its chosen assurance level.

### 1.1.14 Ad Hoc

The Ad Hoc report presents the same information displayed by the Application Detail report; and allows the end-user to limit the information presented based on six criteria:

- Application Name
- Assessment Date
- User Role
- Participants
- User Role Assurance Level
- Transaction Assurance Level

Any of the criteria may be used by the user. However, three of the criteria work together: Application Name, Assessment Date and User Role. These three criteria behave in a hierarchical manner, where Applications limit the available Assessment Dates and Assessment Dates limit the available User Roles. The user does not have to use all three of these criteria, but they must use a higher level criteria before they can use a lower level criteria (e.g. a user who wants to filter based on User Role must filter based on Application Name and Assessment Date first). The remaining three criteria can be used alone or in conjunction with any other criteria. Users perform this filtering by using the AD Hoc Reporting Form.

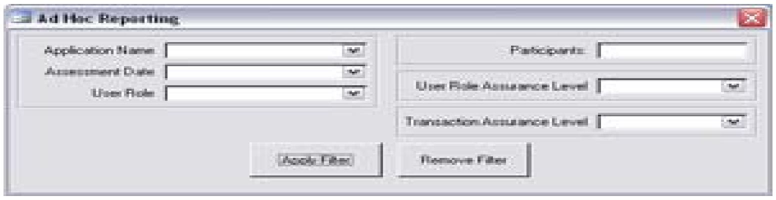


**Figure 16: Ad Hoc Reporting Form**

This form is presented every time the Ad Hoc Report is requested by a user.

# Appendix D: OMB Authentication Guidance

On December 16, 2003, the Office of Management and Budget issued final guidance on authentication for access to electronic transactions on E-Government systems. This guidance is provided in “e-Authentication Guidance for Federal Agencies” and includes specific definitions for four authentication levels, based on the potential risks and impact of unauthorized use of electronic transaction. For convenience, the authentication levels as defined by this OMB guidance are provided below.

## *1.1 Level 1*

### 1.1.1 Definition

Little or no confidence exists in the asserted identity. For example, Level 1 credentials allow people to bookmark items on a web page for future reference.

### 1.1.2 Examples

- In some instances, the submission of forms by individuals in an electronic transaction will be a Level 1 transaction:
    - when all information is flowing to the Federal organization from the individual
    - there is no release of information in return
    - the criteria for higher assurance levels are not triggered
- For example, if an individual applies to a Federal agency for an annual park visitor’s permit (and the financial aspects of the transaction are handles by a separate contractor and thus analyzed as a separate transaction), the transaction with the Federal agency would otherwise present minimal risks and could be treated as Level 1.
- A user presents a self-registered user ID or password to the U.S. Department of Education web page, which allows the user to create a customized “My.ED.gov” page. A third party gaining unauthorized access to the ID or password might infer personal or business information about the individual based upon the customization, but absent a high degree of customization however, these risks are probably very minimal.
- A user participates in an online discussion on the whitehouse.gov website which does not request identifying information beyond name and location. Assuming the forum does not address sensitive or private information, there are no obvious inherent risks.

## *1.2 Level 2*

### 1.2.1 Definition

On balance, confidence exists that the asserted identity is accurate. Level 2 credentials are appropriate for a wide range of business with the public where agencies require an initial identity assertion (the details of which are verified independently prior to any Federal action).

### 1.2.2 Examples

- A user subscribes to the Gov Online Learning Center (www.golearn.gov). The site’s training service must authenticate the person to present the appropriate course material, assign grades, or demonstrate that the user has satisfied compensation-or promotion-related training requirements. The only risk associated with this transaction is a third party gaining access to grading information, thereby harming the student’s privacy or reputation. If the agency determines that such harm is minor, the transaction is Level 2.

- A beneficiary changes her address of record through the Social Security web site. The site needs authentication to ensure that the entitled person’s address is changed. This transaction involves a low risk of inconvenience. Since official notices regarding payment amounts, account status, and records of changes are sent to the beneficiary’s address of record, it entails moderate risk of unauthorized release of personally sensitive data. The agency determines that the risk of unauthorized release merits Assurance Level 2 authentication.
- An agency program client updates bank account, program eligibility, or payment information. Loss or delay would significantly impact him or her. Errors of this sort might delay payment to the user, but would not normally result in permanent loss. The potential individual financial impact to the agency is low, but the possible aggregate is moderate.
- An agency employee has access to potentially sensitive personal client information. She authenticates individually to the system at Level 2, but technical controls (such as a virtual private network) limit system access to the system to the agency premises. Access to the premises is controlled, and the system logs her access instances. In a less constrained environment, her access to personal sensitive information would create moderate potential impact for unauthorized release, but the system’s security measures reduce the overall risk to low.

## *1.3 Level 3*

### 1.3.1 Definition

Level 3 is appropriate for transactions needing high confidence in the asserted identity’s accuracy. People may use Level 3 credentials to access restricted web services without the need for additional identity assertion controls.

### 1.3.2 Examples

- A patent attorney electronically submits confidential patent information to the US Patent and Trademark Office. Improper disclosure would give competitors a competitive advantage.
- A supplier maintains an account with a General Services Administration Contracting Officer for a large government procurement. The potential financial loss is significant, but not severe or catastrophic, so Level 4 is not appropriate.
- A First Responder accesses a disaster management reporting website to report an incident, share operational information, and coordinate response activities.
- An agency employee or contractor uses a remote system giving him access to potentially sensitive personal client information. He works in a restricted-access Federal office building. This limits physical access to his computer, but system transactions occur over the Internet. The sensitive personal information available to him creates a moderate potential impact for unauthorized release.

## *1.4 Level 4*

### 1.4.1 Definition

Level 4 is appropriate for transactions needing very high confidence in the asserted identity’s accuracy. Users may present Level 4 credentials to assert identity and gain access to highly restricted web resources, without the need for further identity assertion controls.

### 1.4.2 Examples

- A law enforcement official accesses a law enforcement database containing criminal records. Unauthorized access could raise privacy issues and/or compromise investigations.
- A Department of Veteran's Affairs pharmacist dispenses a controlled drug. She would need full assurance that a qualified doctor prescribed it. She is criminally liable for any failure to validate the prescription and dispense the correct drug in the prescribed amount.
- An agency investigator uses a remote system giving her access to potentially sensitive personal client information. Using her laptop at client worksites, personal residences, and businesses, she accesses information over the Internet via various connections. The sensitive personal information she can access creates only a moderate potential impact for unauthorized release, but her laptop's vulnerability and her non-secure Internet access raise the overall risk.

# Appendix A:  Document History

| Status | Release | Date | Comment | Audience |
|---|---|---|---|---|
| Approved | 1.0.0 | | 1st release of document | Public |
| Revision | 1.0.1 | 06/14/05 | • Replaced images 1 and 2 with updated screenshots.<br>• Added e-RA User Roles section.<br>• Added User Role Assurance Level section.<br>• Added details on Executive Summary, Application Detail, and Ad Hoc reports in Appendix C.<br>• Made updates to Purpose and Use of e-RA Tool, Glossary, and Appendix B to reflect the tools new reliance on user roles.<br>• Made updates to all Activity sections (4-13) as they relate to user roles, mitigation, and highest vs. chosen assurance levels. | Limited |
| Revision | 1.0.2 | 06/15/05 | • Replaced initiative with application or agency throughout document.<br>• Corrected spelling of E-Authentication in section 1.<br>• Moved footnotes 1 and 2 to the footer.<br>• Changed screenshot titles from images to figures.<br>• Added bullets to lists throughout document.<br>• Added activity screenshots to sections 4-13.<br>• Renumbered lists throughout document where necessary.<br>• Corrected spelling of E-Government throughout document.<br>• Moved glossary to Appendix A.<br>• Made appropriate grammatical changes and terminology updates throughout document.<br>• Placed document into proper E-Authentication format. | Limited |
| Revision | 1.0.3 | 06/22/05 | • Expanded section on Ad Hoc Reporting to incorporate information related to the Ad Hoc Reporting Form.<br>• Moved document history to Appendix A.<br>• Removed Acknowledgement section. | Limited |
| Release | 1.1.0 | 07/06/05 | Delivered to PMO for approval. | PMO |
| Revision | 1.5 | 10/18/05 | • Changed version to 1.5 to be consistent with the version of the e-RA tool.<br>• Removed version of tool throughout document where appropriate.<br>• Added “Before Using e-RA” section 2.2 detailing naming conventions an initial setup.<br>• Added “Importing and Exporting Data with e-RA” section 14 and its subsections detailing how to export from 1.5 to Excel, as well as the functional and technical reasons for not importing data into the e-RA databases. | Public |