Table of Contents

Session 2 Introduction
Session 2 Welcome and Overview ................................................................. 2-1

Take-Home Activity Debrief
Session 1 Activity: Determine Essential Functions and Identify Essential Records—Part 2 ................................................................. 2-3

Module 2—Protect Essential Records

Module 2 Introduction and Objectives
Module 2 Introduction ..................................................................................... 2-7
Module 2 Objectives ......................................................................................... 2-8

Lesson 1: Identify and Evaluate Hazards and Risks
Risk Management Key Terms ......................................................................... 2-10
Risk Assessment—Identify Risks .................................................................... 2-12
Risks From Loss of Agency Memory ............................................................... 2-13
Risks Related to Emergencies ........................................................................ 2-14
Risks Related to Records Management ......................................................... 2-16
Scope of an Emergency or Disaster ............................................................... 2-18
Risk Assessment Factors .............................................................................. 2-19
Risk Assessment Techniques ......................................................................... 2-20
Risk Analysis—Evaluate Risks ....................................................................... 2-22
Managing the Risk: Prioritizing Actions ......................................................... 2-31
Document the Risks ......................................................................................... 2-32

Session 2 Review and Wrap-Up
Session Review ............................................................................................... 2-35
Activity: Identify and Evaluate Risks ............................................................. 2-36
Session 2 Introduction

Session 2 Welcome and Overview

Slide 2-1

Join the conference call by dialing the conference number in your Invitation or Reminder Emails. Please put your phone on mute.

Be sure to have all Session 2 materials ready before the session starts. You’ll find the link to the materials in your Invitation or Reminder Emails.

Required materials for Session 2:

- Session 2 Participant Guide
- Session 2 handouts:
  - Handout 2.1—Risk Assessment—Sample Hazards Inspection Checklist
  - Handout 2.2—Possible Hazards
  - Handout 2.3—Identify and Evaluate Risks Activity
- Materials from prior sessions:
  - Handout 1.6—The Division of Public Recreation (DPR) Overview
  - Handout 1.7—Determine Essential Functions and Identify Essential Records Activity, with Tables 1 and 2 completed
Session 2 Overview

- Take-Home Activity Debrief
- Module 2—Protect Essential Records
  - Lesson 1: Identify and Evaluate Hazards and Risks
Take-Home Activity Debrief

Session 1 Activity: Determine Essential Functions and Identify Essential Records—Part 2

Slide 2-3
Module 2—Protect Essential Records
[This page intentionally left blank.]
Module 2 Introduction and Objectives

Module 2 Introduction

Slide 2-4

Module 2—Protect Essential Records
Introduction and Objectives
Module 2 Objectives

At the completion of this module, you will be able to:

- Assess and analyze risks to essential records, including risks specific to your region or locality
- Identify and evaluate preparedness and mitigation measures
Lesson 1: Identify and Evaluate Hazards and Risks

Module 2—Protect Essential Records

Lesson 1: Identify and Evaluate Hazards and Risks
You need to be familiar with certain terms in order to discuss protection of your essential records:

- **A hazard** is something that is potentially dangerous or harmful, often the root cause of an unwanted outcome. Hazard is the term used by DHS/FEMA to describe a natural or manmade incident that creates a risk. An example of a hazard would be overhead pipes in a file room.

- **Risk** is the potential harm that may arise from some present process or future event. Examples of risks encountered in records management include damage to records, records getting wet from an overhead pipe leak, and unauthorized destruction of records.

- **Risk management** is the entire process of assessing risks, evaluating risks, and then deciding on priorities for actions and informing the agency, so that resources are available and actions can be taken to manage the risk. What we are doing in risk management for essential records entails developing a strategy to manage the risks by identifying and evaluating protection strategies appropriate for essential records. Examples of risk management include storing records in waterproof cabinets, inspecting pipes annually, and relocating records stored in risky environments.

- **Risk assessment** is an examination of the potential harm that may result from exposure to certain hazards. Simply put, risk assessment is the identification of risks. An example of risk assessment would be taking a closer look at the file room where your records are stored, and determining what harm to the records might occur if the overhead pipes in your file room leaked.
**Risk analysis** is the systematic use of available information to determine how often specified events may occur and the magnitude of the consequences if they do occur. We use risk analysis to evaluate the probability of occurrence of the risk identified in the risk assessment, and the impact the occurrence of those risks would have on your records and information.

For example, in your risk assessment, you determined that the overhead pipes in your file room represent a risk: They could spring a leak and damage the records. During the risk analysis, you would determine the probability of a leak’s occurring and the impact it would have on the records.

When planning your essential records program, you will use risk assessment and analysis to:

- Identify the risks involved if the essential records remain in their current locations and on their current media
- Identify the difficulty of reconstituting the records if they are destroyed
- Determine whether off-site storage is necessary
- Determine whether use of alternative storage media is advisable
- Determine whether it is necessary to duplicate records to provide an essential record copy
In order to identify risks properly, you must first be aware of the types of risk you may encounter. The risks relevant to an essential records program can be grouped into three categories:

- Risks from loss of agency memory
- Risks related to emergencies
- Risks related to records management

To list all possible types of risks pertaining to essential records would be impossible. Every records management program is different and faces its own unique types of risk. The risks included in these three categories may or may not apply to your essential records program, but they should serve as a starting point to get you thinking about the risks faced by your program.
The loss of agency memory is the absence of valuable program and/or administrative information (background information, current data, and/or historical references)—an absence or lack that can result in poor decisions, incorrect information given to residents, and the loss of a historical record.

There are two types of agency memory loss:

- **Physical loss** of records or information
- **Intellectual loss**, including loss of intellectual control. When agency employees maintain information on their individual desktop computers rather than in a centralized location, agencies often have no control over—or idea of—what information exists and where it is located.
Risks Related to Emergencies

Slide 2-10

Records emergencies can be devastating to an agency. If the emergency is severe enough, or the loss of records and information critical, it is likely that the agency may not be able to recover. A very severe emergency that overpowers an agency’s or community’s ability to respond is termed a disaster.

Records emergencies can be categorized as follows:

- Natural emergencies
- Technological emergencies
- Civil emergencies

These emergencies often interact, one influencing or aggravating another. We present them separately here to raise awareness of the risks of each.
Natural Emergencies

- Earthquakes
- Hurricanes
- Tornadoes
- Floods

Technological Emergencies

- Building and equipment failures
- Electrical malfunctions
- Hazardous material accidents
- Airplane crashes

Civil Emergencies

- Arson
- Widespread theft and looting
- Vandalism
- Terrorism
- War
There are several types of risks related to records management:

- **Legal**—Risk of losing a legal challenge because the agency may not have created or maintained records necessary to prove its case. Poor management of records may make the agency unable to respond to a request for access under legal discovery, the Freedom of Information Act, open records, or right-to-know laws. Retaining many records for long periods increases the number of records that an agency must sort through in response to such requests.

- **Security**—Inadequate physical and network security measures increase the risk of loss or alteration of records. Also, there is a risk of restricted information, such as confidential or Privacy Act information, being released inappropriately.

- **Business**—Risk of bad decision-making without necessary records, and of the poor organization of records hindering daily operations, rendering the program ineffective.
• **Accountability**—Risk of not being able to satisfy public scrutiny, of not being able to provide full government accountability, and of not being able to respond to requests for access to restricted records, because records are not created or maintained appropriately.

• **Technology**—Risk of losing data or not being able to access data, due to changes in technology.
  - Records stored on individual hard drives are not backed up with the network, so if the hard drive crashes, the records could be lost irretrievably.
  - Technological obsolescence—Rapid changes in hardware and software formats and media put records at risk, because the agency might not be able to open and read records in the future.

• **Long-term preservation of records**
  - Environment—Environmental conditions such as excessive heat, humidity, sunlight, etc., increase the risk that the physical media on which the records are stored will deteriorate.
  - Physical format deterioration—The longer records are kept, the greater the risk of records being lost because the physical format degrades over time, because of inherent instability in media such as floppy disks, factors like acid in paper, etc.
The scope of a disaster or emergency is also an important factor to consider when identifying risks. The scope can be either:

- **On site**—Events with a very narrow scope, striking only a single building, floor, or office. Use of community and organizational resources is possible. Response and recovery can begin quickly. Examples include fires, burst water pipes, or power failures.

- **Immediate vicinity**—Events in which loss of life, power outages, and massive destruction may occur, but communication and emergency services are typically not affected. Typically, backup procedures can be applied immediately, but records salvage may be hindered. Examples include tornadoes or bombing incidents.

- **Community- or region-wide**—Events with immediate disruption of communications and emergency services, power outages, and widespread destruction. Employees’ homes and families are often endangered. Access to and restoration of backup information is often hindered. Getting to facilities and work sites to begin records and information recovery can be difficult. Examples include hurricanes and other widespread natural emergencies.
Risk Assessment Factors

As you assess the risks to your agency and its records, you should consider the following factors:

- **Existing risks to records**—Are any of your agency’s essential records already at risk? Are the records stored under appropriate security and environmental conditions? Will the technology you need to access and read the records be available? Are any of the records in a format that is difficult to duplicate and secure off site?

- **Physical location of the essential records**—Consider your site’s physical location and characteristics. What is the building like? Is it located in a high-traffic area, a flood plain, or near other hazardous sites? Is it prone to any locality-specific risks, such as certain weather events? Are the records stored in a basement or an attic?

- **Security and controls already in place**—What security and access controls are already in place? Consider not just the controls related to securing your building and storage areas (e.g., locks, fire detection), but also security and access controls for electronic systems.

- **Vulnerable areas**—As you assess the current situation for your agency, identify the vulnerable areas that need to be addressed to minimize risk.

- **Timing**—It can also be worthwhile to examine how the risks differ, depending on whether an incident occurs during working hours or non-working hours. Agencies may assume that they’ll have sufficient personnel available to respond to an incident during working hours, but what if an incident occurs during non-working hours? Will they still have sufficient personnel available to respond?
Risk Assessment Techniques

There are many different techniques for identifying risks. Not all will be applicable to smaller communities and agencies. For some, interviews or brainstorming may be the best option. Nevertheless, find the best way for your agency, but definitely conduct a risk assessment. Three common techniques are:

- Physical site survey
- Expert interviews
- Brainstorming

**Physical Site Survey**

The physical site survey provides information on additional specific risks to the location(s) in which essential records are kept. Begin the survey up to a mile out and work inwards to the building noting all possible dangers; then assess the building itself.

A team or a committee carries out a physical survey of locations where essential records are stored, along with a review of security procedures already in place. Information that can be gathered by the survey includes:

- Number and types of employees who have access to the essential records
- Proximity of storage areas to laboratories, factories, or other facilities that contain flammable materials or hazardous substances
- Vulnerability to water damage
• Availability of fire control apparatus (detection, suppression, etc.) and fire department services

• Ability to reconstruct recorded information through backup procedures or use of other media

(Refer to Handout 2.1—Risk Assessment—Sample Hazards Inspection Checklist for an example of some of the hazards you might look for in a physical survey.)

**Expert Interviews**

Expert interviews are the easiest and most frequently used risk identification technique, with the caveat that the quality depends on the interviewer’s being unbiased. This technique provides a way to collect risk-related data from subject matter experts and other stakeholders. It relies on expert judgment to identify and analyze potential risks, and to develop strategies to address them.

Information from local sources might highlight elements of risk that are unknown to your agency. You may discover that your building was once the site of a flood, and that all the damage has been cleaned up so that the effects are not visible. Your fire patrol and facilities staff could help you identify whether there is a risk of an arson attack.

You should also discuss risks with your emergency management agency and information technology (IT) staff. Others who could provide useful insights include experts on flooding, earthquakes, and public health issues.

Hazards are seldom deeply held secrets. Experience indicates that virtually all risks of significant impact are more or less common knowledge. Therefore, the challenge lies in gathering the knowledge of that hazard so that the risk can be managed.

**Brainstorming**

For information on risks specific to your agency, brainstorming unearths and documents your in-house expertise. The goal of the brainstorming technique is to help people search creatively for hazards and risks, and to stimulate thinking outside the box.

Brainstorming is a group process. Each member of the group is asked to provide input on major issues leading to risks. Members are encouraged to use each other’s ideas to generate new ideas. The results of this discussion are summarized as the group’s results, and risk issues are identified.

To assist with the brainstorming, expert judgments for local events can be found on websites, including those of NOAA (National Oceanic and Atmospheric Administration), USGS (U.S. Geological Survey), and DHS/FEMA, for the United States. In general, hazards from natural phenomena are ranked by state, and may include projections for future events.

Refer to **Handout 2.2**—Possible Hazards for a list of events that may be a risk to your essential records.

Refer to the Intergovernmental Preparedness for Essential Records (IPER) Resource Center, located at [http://www.statearchivists.org/resource-center](http://www.statearchivists.org/resource-center) for resources on identifying risks that are relevant to your state.
Once you’ve identified the risks to your essential records, your next step is to evaluate those risks by performing a risk analysis. As mentioned earlier, risk analysis evaluates the probability and the impact of identified risks. The purpose of the risk analysis is to identify where and how to direct your efforts and resources. Smaller agencies should review the options presented here and adapt them to their own needs. Some form of risk evaluation is very important.

A risk analysis consists of three steps:

1. Establish a rating system:
   - Probability rating
   - Impact rating
2. Rate your risks.
3. Evaluate your findings.
Step 1: Establish Your Rating System

A risk analysis should include an appropriate method of scoring risks and impacts. Each risk you identified in your risk assessment should be rated on two criteria:

- What is the likelihood (probability) of such an incident occurring?
- What impact would it have on your operations?

Therefore, your rating system should contain two ratings:

- A probability rating
- An impact rating

A simple approach is to measure these as high, medium, or low. However, you can also use a numerical scale (for example: 1–3, 1–5, 1–10), if you prefer.

It’s important to point out that there is no one-size-fits-all rating system. Your rating systems should be based on your professional experience, your best judgment, and/or the experience of consultants.
Probability Rating

Create your probability rating by selecting the rating scale you wish to use (high-low, numerical, etc.) and defining the criteria for the ratings.

A sample probability rating is shown in the table below.

<table>
<thead>
<tr>
<th>PROBABILITY RATING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SCALE</strong></td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>Low</td>
</tr>
</tbody>
</table>

Note that the likelihood of the event occurring within a certain time period is a factor in estimating its probability. For example, you could decide in your rating system that an event that is not likely to occur within 10 years has a low probability rating.

Thus, you are not only deciding on a rating system, you are also deciding on a standard for what your ratings mean.
Step 1: Establish a Rating System (cont’d.)

Impact Rating

<table>
<thead>
<tr>
<th>Scale</th>
<th>Criterion</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Catastrophic impact; devastating loss.</td>
</tr>
<tr>
<td>Medium</td>
<td>Serious/critical impact; significant loss.</td>
</tr>
<tr>
<td>Low</td>
<td>Minor/marginal impact; some loss.</td>
</tr>
</tbody>
</table>

Impact Rating

Create your impact rating just as you did the probability rating: select the rating scale you wish to use (high-low, numerical, etc.) and define the criteria for the ratings.

Base your criteria on the financial and program implications of the risk event, such as:
- The cost to reconstruct lost or damaged records
- The probability of compromising an agency’s program objectives
- The possibility of generating a lawsuit

A sample impact rating is shown in the table below.

Table 3: Sample Impact Rating

<table>
<thead>
<tr>
<th>Scale</th>
<th>Impact Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Catastrophic impact; devastating loss</td>
</tr>
<tr>
<td>Medium</td>
<td>Serious/critical impact; significant loss</td>
</tr>
<tr>
<td>Low</td>
<td>Minor/marginal impact; some loss</td>
</tr>
</tbody>
</table>
Step 1: Establish a Rating System (cont’d.)

- Compile ratings to create your rating system

<table>
<thead>
<tr>
<th>Probability of Risk</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact of Risk</td>
<td>Catastrophic impact, devastating loss</td>
<td>Catastrophic impact, devastating loss</td>
<td>Catastrophic impact, devastating loss</td>
</tr>
<tr>
<td></td>
<td>The event has little chance of occurring.</td>
<td>Similar events have occurred in the past.</td>
<td>The event is expected to occur.</td>
</tr>
<tr>
<td></td>
<td>Serious/critical impact, significant loss</td>
<td>Serious/critical impact, significant loss</td>
<td>Serious/critical impact, significant loss</td>
</tr>
<tr>
<td></td>
<td>The event has little chance of occurring.</td>
<td>Similar events have occurred in the past.</td>
<td>The event is expected to occur.</td>
</tr>
<tr>
<td></td>
<td>Minor/marginal impact, some loss</td>
<td>Minor/marginal impact, some loss</td>
<td>Minor/marginal impact, some loss</td>
</tr>
<tr>
<td></td>
<td>The event has little chance of occurring.</td>
<td>Similar events have occurred in the past.</td>
<td>The event is expected to occur.</td>
</tr>
</tbody>
</table>

Rating System

Once you’ve established your rating scales, compile the scales into a single table to create your rating system. A sample rating system is provided below.
### Table 4: Example—Risk Analysis Rating System

<table>
<thead>
<tr>
<th>Impact of Risk</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low</strong></td>
<td>Minor/marginal impact; some loss</td>
<td>Minor/marginal impact; some loss</td>
<td>Minor/marginal impact; some loss</td>
</tr>
<tr>
<td>The event has little chance of occurring</td>
<td>Similar events have occurred in the past</td>
<td>The event is expected to occur</td>
<td></td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>Serious/critical impact; significant loss</td>
<td>Serious/critical impact; significant loss</td>
<td>Serious/critical impact; significant loss</td>
</tr>
<tr>
<td>The event has little chance of occurring</td>
<td>Similar events have occurred in the past</td>
<td>The event is expected to occur</td>
<td></td>
</tr>
<tr>
<td><strong>High</strong></td>
<td>Catastrophic impact; devastating loss</td>
<td>Catastrophic impact; devastating loss</td>
<td>Catastrophic impact; devastating loss</td>
</tr>
<tr>
<td>The event has little chance of occurring</td>
<td>Similar events have occurred in the past</td>
<td>The event is expected to occur</td>
<td></td>
</tr>
</tbody>
</table>

**Probability of Risk**

- Low
- Medium
- High
Step 2: Rate Your Risks

Once you’ve established your rating system, your next step is to rate each risk identified in your risk assessment:

- Rate the probability of the risk event occurring using your probability rating.
- Rate the impact of the risk event occurring using your impact rating.

Example:

The procurement office on the second floor has 10 file cabinets containing essential records that are located within two feet of inoperable windows. Outside the windows is a large oak tree. The windows have been broken in the past during a major storm. The office also houses several servers in an area that is not secure from unauthorized access. The fire suppression system is not appropriate to IT equipment (it is water-based) and there is a lack of equipment redundancy (so that failure of a single disk is catastrophic). Phone and data connections are located next to the windows.

A risk assessment has been performed, and the following risks have been identified:

1. Debris blocking access to cabinets
2. Debris and water from storm
3. Mold and mildew
4. Temperature and humidity—unstable environment
5. Loss of data
6. Fire damage
7. Inability to access data
8. Inability to communicate
Slide 2-21

### Step 2: Rate Your Risks (cont’d.)

<table>
<thead>
<tr>
<th>Identified Risk</th>
<th>Probability</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debris blocking access to cabinets</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Debris and water from storm</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Mold and mildew</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Temperature and humidity—unstable environment</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Loss of data</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Fire damage</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Inability to access data</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Inability to communicate</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>

Table 5: Example—Rating Your Risks

<table>
<thead>
<tr>
<th>IDENTIFIED RISK</th>
<th>PROBABILITY</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debris blocking access to cabinets</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Debris and water from storm</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Mold and mildew</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Temperature and humidity—unstable environment</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Loss of data</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Fire damage</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Inability to access data</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Inability to communicate</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>

Keep in mind that your risk situation can change at any time, so it’s important to review and update your risk ratings periodically. For instance, with regard to the probability of an event, just because something has not occurred in the past doesn’t mean it can’t happen in the future. Changes such as renovations that reroute water pipes may suddenly raise or lower the risk to your records storage area.
Step 3: Evaluate Your Findings

Once you’ve rated the risks to your essential records, your next step is to evaluate your findings. This evaluation will help you determine where to direct your efforts and resources for protecting your essential records.

To conduct the evaluation, return to your rating system and determine your threshold for action: Which probability and impact combinations require action to protect the records and reduce the risks, and which do not? For example, obviously, the risks with high probability and high impact require action, but what about risks with high impact and low probability? Or risks with medium probability and medium impact? Do they also require action, or can you accept these risks? These are decisions that will be unique to your agency, based on your needs and resources.

Once you’ve determined your threshold for action, apply this to your risks and identify which risks require action and which do not.
Managing the Risk: Prioritizing Actions

• To prioritize your actions, rank the risks that require action.
• When prioritizing, consider:
  – Cost to reconstruct the data
  – Cost of defending against legal actions associated with loss

After you have analyzed the risks to your agency’s essential records and arrived at which risks require action, you need to rank these risks to prioritize your actions. Setting these priorities for your planning and protection efforts is part of managing the risk. As you prioritize the risks, you should consider:

• The cost to reconstruct the data. This should not only include the number of staff hours involved in recreating the records if they are lost, but should also take into consideration the value of lost business, revenue, and goodwill.

• The cost of defending against legal actions associated with loss
Document the Risks

Document the results of your risk assessment, risk analysis, and prioritizing is the final step before action. It enables you to prepare a strategy for communicating the risks to your agency so that the agency can take appropriate action. Your risk priorities can be addressed as part of COOP (Continuity of Operations) planning, essential records program planning, emergency planning and records management, and information technology planning.

Include the following information in your documentation:

- Potential risk—List the risk itself. For example, the agency might face a risk of water damage to its records.

- Source of risk—Record the potential source(s) of the risk. For example, the water damage might be caused by a leaky roof.

- Location of impact—Record where the risk will have an impact. Agency-wide? One particular part of the building? One work process or function? One system?

- How probable is an incident?—Rate the probability of the risk occurring. For example, in a rainy area, the likelihood of a roof leak that damages the records might be greater, and therefore have a higher rating, than in a desert area.
- Potential effects on essential records—List the potential effects of the risk on your essential records. For example, mold and mildew might begin to grow on waterlogged records.

- Severity of impact—Rank the severity of the impact to the records, if the effect were to occur.

- Existing control measures—Record any current steps, processes, or strategies your agency has in place to detect the presence of a risk, prevent it from happening, and/or mitigate its effect.

- Be sure also to include the rating system used in your risk analysis, so your readers will understand what the ratings mean.

NOTE: The risk matrix that you’ll prepare in this session’s activity is one example of how to document the process and use it to compile a list of recommended actions, which in turn will assist the agency in planning for an essential records program and identifying the resources it will need.
[This page intentionally left blank.]
Session 2 Review and Wrap-Up

Session Review

In Session 2, you learned:

- Several risk management key terms
- Risk assessment
  - Categories of risks
  - Factors to consider when identifying risks
  - Techniques for identifying risks
- Risk analysis
- Prioritizing and documenting risks
Activity: Identify and Evaluate Risks

Slide 2-26

Activity materials:

- **Handout 1.6**—The Division of Public Recreation (DPR) Overview
- **Handout 1.7**—Determine Essential Functions and Identify Essential Records Activity
- **Handout 2.3**—Identify and Evaluate Risks Activity
Slide 2-27

Materials for Part 1 of the Activity

Handout 1.6

Handout 1.7—Table 1:
DPR Essential Functions and
Essential Records

Handout 2.3—Table 1:
DPR Risk Matrix

Slide 2-28

Materials for Part 2 of the Activity

Handout 2.3—Table 3:
My Agency’s Risk Matrix

Handout 1.7—Table 2:
My Agency’s Essential Functions
and Essential Records
Thank You!