Essential Records Webinar

Session 3

Instructor Guide

Final, July 2010

Course Number: AWR-210-2

Table of Contents

Session 3—Administration Page

Duration

90 minutes

The following is a suggested time plan for this session. We encourage the instructor to adapt it as needed.

The blank “Start Time” column exists as a worksheet on which you can create a schedule for your specific session. Using the scheduled start time of your session and the suggested durations provided in Table 1, calculate the start time of each topic and enter it in the “Start Time” column. Also record the start times in the blank Start Time fields provided throughout this document, at the beginning of the topics. This will help you keep track of your progress and help you check whether or not you’re on schedule.

Table 1: Suggested Time Plan

Topic	Duration	Start Time
Session 3 Introduction		
• Session 3 Welcome and Overview	5 minutes	
Take-Home Activity Debrief		
• Session 2 Activity: Identify and Evaluate Risks—Part 2	20 minutes	
Module 2—Protect Essential Records		
• Introduction and Objectives	5 minutes	
• Lesson 2: Determine and Evaluate Preparedness and Mitigation Strategies	30 minutes	
Session 3 Review and Wrap-Up		
• Session Review	5 minutes	
• Activity: Determine Protection Strategies and Measures	25 minutes	
Total Duration	**90 minutes**	

Scope Statement

Session 3 addresses the selection and evaluation of preparedness and mitigation strategies to protect essential records, such as prevention and mitigation actions, dispersal, vaulting, and storage. It includes:

- Session 3 Introduction
- Take-Home Activity Debrief
- Module 2—Protect Essential Records:
  - Lesson 2: Determine and Evaluate Preparedness and Mitigation Strategies
- Session 3 Review and Wrap-Up

Session 3 Introduction

The Session 3 Introduction quickly reviews the material covered in prior sessions and previews the material to be covered in Session 3.

Take-Home Activity Debrief

The Take-Home Activity debrief provides participants with the opportunity to share the results of their homework assignment with the class, receive feedback from the instructors, and discuss any issues or questions they may have about the activity.

Module 2

NOTE: Module 2 is split between Session 2 and Session 3:

- Lesson 1 is presented in Session 2.
- Lesson 2 is presented in Session 3.

Lesson 2 of Module 2 focuses on identification and evaluation of preparedness and mitigation strategies for essential records. It begins by examining two strategies to handle risk: acceptance and mitigation. It also discusses various strategies to protect essential records, and options for storage of essential records. The lesson addresses planning for the availability of essential records, and provides a review of the issues that should be considered when evaluating protection strategies.

Session 3 Review and Wrap-Up

The Session 3 Review and Wrap-Up quickly reviews the key points covered in Session 3 and introduces the material to be covered in Session 4. It also introduces the Take-Home Activity.

Session Objectives

Module 2—Protect Essential Records

NOTE: As mentioned above, Module 2 is presented across two sessions. The objectives addressed in this session appear below bold.

Terminal Learning Objectives:

- Participants will be able to identify and evaluate risks to the essential records of an agency.
- **Participants will be able to identify and evaluate preparedness and mitigation strategies to protect and ensure continued access to essential records in case of natural disasters or human-caused threats such as arson, vandalism, computer hacking, or terrorism.**

Enabling Objectives:

- Assess and analyze risks to essential records, including risks specific to your region or locality
- **Identify and evaluate preparedness and mitigation measures**

Instructor-to-Participant Ratio

2:30—We suggest that at least two instructors lead each webinar and that there be no more than 30 participants.

Methods

The following instructional methods are used in this session:

- Instructor presentation
- Group discussion
- Polling question
- In-Session Activity
- Take-Home Activity

Practical Exercise

Session 3 contains one two-part activity, Determine Protection Strategies and Measures, in which participants identify protection strategies and measures to address risks to essential records.

- Part 1 is an In-Session activity focusing on a fictitious state agency.
- Part 2 is a Take-Home Activity focusing on the participant's own agency.

Sources of Course Content

- National Archives and Records Administration's (NARA) course, Vital Records (April 2008)
- National Institute of Standards and Technology's (NIST) publication **Contingency Planning Guide for Federal Information Systems**. SP 800-34 Rev. 1 (May 2010) *http://www.csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1.pdf*

Instructional Materials

- Session 3 Instructor Guide (for instructors)
- Session 3 Participant Guide (for participants)
- Session 3 Slides
- Handout(s):
  - **Handout 1.6**—The Division of Public Recreation (DPR) Overview
  - **Handout 2.3**—Identify and Evaluate Risks Activity
  - **Handout 3.1**—Protection Strategies Based on Media Requirements
  - **Handout 3.2**—Determine Protection Strategies and Measures Activity

- Reference(s):
  - **Reference 01**—Resource Center, References, Reading List
  - **Reference 02**—Key Terms for the IPER Courses
  - **Reference 03**—Participant Webinar Reference Guide
  - **Reference 04**—iLinc Quick Reference for IPER Instructors (instructors only)
  - **Reference 05**—Webinar Troubleshooting Guide (instructors only)
- Polling question(s):
  - None
- Prepared Powerboard file(s):
  - **PB 3.1**—Session 3 Review
- Evaluation(s):
  - None

Equipment

- Required equipment:
  - Internet-enabled computer
  - Telephone (Each instructor should have his or her own telephone. If you want to use the telephone hands-free, you should use a headset instead of a speakerphone to reduce background noise that will distract the participants.)
- Optional equipment:
  - A second Internet-enabled computer, logged into the webinar as a participant, so you can see what the participants see.

[This page intentionally left blank.]

Session 3 Introduction

Instructor Notes	Participant Guide
PG 3-1	**Session 3 Welcome and Overview**

PG 3-1

(Duration: 5 minutes)

START TIME: ______________

Log in to iLinc 30 minutes prior to the start of the webinar session to make sure there are no technical issues.

Launch the Session 3 slides file in iLinc.

Show slide 3-1.

Session 3 Welcome and Overview

Required materials for Session 3:

- Session 3 Participant Guide
- Session 3 handouts:
  - **Handout 3.1**—Protection Strategies Based on Media Requirements
  - **Handout 3.2**—Determine Protection Strategies and Measures Activity

- Materials from prior sessions:
  - **Handout 1.6**—The Division of Public Recreation (DPR) Overview
  - **Handout 2.3**—Identify and Evaluate Risks Activity, with Tables 1 and 3 completed

REMINDERS TO INSTRUCTOR:

- Before class begins, ***be sure to check*** (1) the IPER Resource Center for special announcements to Instructors about the course and (2) the Frequently Asked Questions (FAQs) to see if there are any newly posted items that may be relevant to your course or participants.
- When you are not speaking to the participants, ***remember to have*** your phone on mute.
- When you are speaking to the participants, ***remember to reduce or eliminate*** background noises, such as pages being turned, co-workers talking, etc.
- If you are recording this session, ***remember*** that discussions conducted via iLinc's Chat tool are captured in the session recording. When using the Chat tool, ***make sure to maintain*** a professional dialog that is appropriate for everyone to view.

Continue to show slide 3-1 until all participants have joined the session (or until it's time to start the webinar).

- When using iLinc's WebSync function, participants cannot see any actions you perform (such as moving your cursor or scrolling); therefore, when you interact with a web page or document, you will need to provide instructions to the participants on what to do ("scroll down," "select this," etc.) so their view will match your view.

Welcome participants as they enter the webinar.

- ***Tell*** them that the webinar will begin shortly.

Five minutes prior to the start of the session, ***check*** the Attendee panel in iLinc and compare it to the class roster to see if all of the participants have entered the webinar.

If all of the participants have entered:

- ***Say:*** Hi, everybody. This is <your name>. I know it's a couple of minutes early, but since everybody's here, I'd like to get started, if that's OK with everyone.

- ***Begin*** the session (see the "Begin the Session" Instructor Note below).

If all of the participants have not yet entered:

- ***Say:*** Hi, everybody. This is <your name>. We are waiting for a few more people to join us, and then we'll get started.

- ***Monitor*** the Attendee panel until all participants have entered the session or until the start time is reached.

Begin the session (see the "Begin the Session" Instructor Note below).

BEGIN THE SESSION:

Start the iLinc recorder.

Say:

- Welcome to Session 3 of the *Essential Records Webinar*.

- To refresh your memory, I'm <your name> and teaching with me today is <name of Instructor 2>.

- Before we get started, I'd like to remind everyone to mute their phones and not to put your phone on hold during the webinar. If you need to take another call or a break during the session, please hang up and call back to rejoin.

Remind participants that they should have the Session 3 course materials ready (either printed or open on their computer) so they can access them when needed.

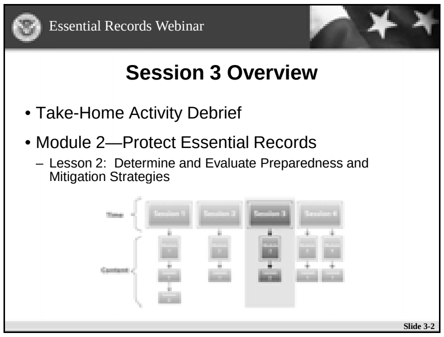
- ***Remind*** participants that the Reminder Email provided a link to the materials.

Say: We don't recommend that you print the materials now, but if you do, please make certain your phone is on mute.

Remind participants that recordings of the sessions are available on the IPER Resource Center, and if they missed the prior session, they can view a recorded version at: *http://www.statearchivists.org/resource-center*

**Transition:** Let's do a quick review of what we covered in our past sessions and take a look at what we're going to discuss today.

Show slide 3-2.



Say:

- In Session 1, we learned how to identify your essential records.
- And last week, in Session 2, we focused on identification and evaluation of the risks to your essential records.

- We defined several risk management terms and examined risk assessment, the identification of risks.
- We also examined risk analysis, the evaluation of risks, and learned the steps to perform a risk analysis.
- Then we took a look at prioritization and documentation of risks.

Go over what will be covered in Session 3:

- ***Say:*** Today, we will focus on how to protect your essential records by identifying and evaluating preparedness and mitigation strategies.
- ***Say:*** The session is comprised of the following:
  - ***Read*** the Session 3 Overview, as provided on the slide.

Say: Today's session is 1 hour and 30 minutes in duration. Because it's a shorter session, there will not be a break.

Take-Home Activity Debrief

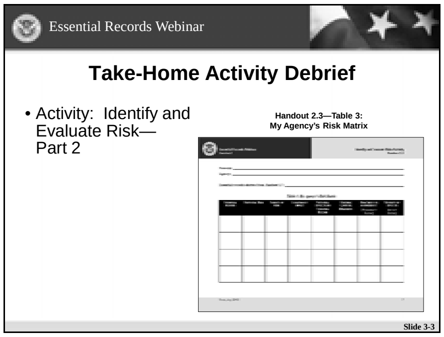
PG 3-3

Session 2 Activity: Identify and Evaluate Risk—Part 2

(Duration: 20 minutes)

START TIME: ______________

Show slide 3-3.



Tell participants to go to **Handout 2.3** (from the Session 2 materials) and locate Table 3: My Agency's Risk Matrix on page 7.

- ***Remind*** participants that this is the table they should have completed for Part 2, the take-home portion, of the Session 2 activity and emailed to you by yesterday.

Ask participants to raise their hands (or use the "Public" tab of the Chat tool) if they had any difficulties completing the Take-Home Activity.

- If anyone had a problem, ***make sure to resolve it*** before continuing.

Debrief the activity by conducting a group discussion:

- ***Say:*** The goal of this activity was to practice identifying, evaluating, and documenting the risks for essential records from your agency. Using two of the essential records you identified in the Session 1 Take-Home Activity, you were asked to complete the Risk Matrix table.

- ***Say:*** I need a volunteer to share their answers for **one** of the risks they identified.

- ***Tell*** participants to share the following:
  - A brief description of the essential record they selected
  - A risk they identified for that record
  - All the associated risk-related information (location, cause, probability, and so forth…)

- ***Tell*** participants to raise their hands to answer or to type their answers in the Chat tool, using the "Public" tab.
- ***Call on*** participants who have their hands raised.
  - ***Remind*** participants to take their phones off mute before speaking.
- ***Acknowledge*** any responses provided in the Chat tool.
- ***Confirm or correct*** responses as appropriate.
- OPTIONAL: If no participants volunteer, you may opt to share a response from one of the homework sheets submitted by the participants.

Continue to debrief the activity in the same manner.

- ***Have*** at least three participants share a risk they identified.
- ***Make sure*** different participants share, so the same few don't do all the talking or chatting.

Once you have completed the debriefing, ***point out*** the following:

- When developing a risk matrix, it's not necessary to come up with a separate table for each essential record.

- If the essential records are in the same format and in the same location they can be grouped together in the same row (the column info will be the same for all, as long as medium and location are the same).
- Keep in mind that within a building, some areas may pose a higher risk than others.

Ask for and resolve any questions.

Remind participants why it is important to do the homework, as assigned. The activities are designed to:

- Apply what was discussed in a particular session
- Build on each other
- Take you through the initial steps of identifying and protecting your essential records

Transition: As we mentioned in Session 2, a risk analysis helps you prioritize and plan the prevention and mitigation strategies for your essential records. Let's pick up with the second half of Module 2, where we'll focus on identification and evaluation of protection strategies.

Module 2—
Protect Essential Records

[This page intentionally left blank.]

Module 2 Introduction and Objectives

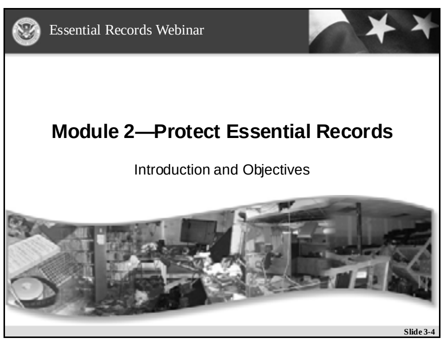
PG 3-7

Module 2 Introduction

(Duration: 5 minutes)

START TIME: ______________

Show slide 3-4.



Introduce the module:

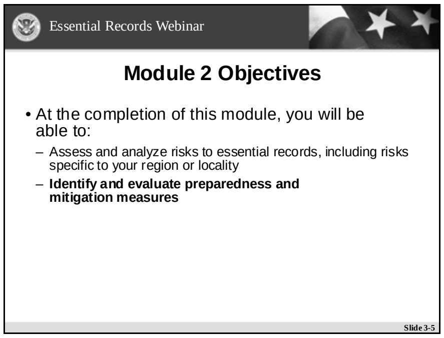
- ***Remind*** participants that Module 2 contains two lessons, which are presented across two sessions. In last week's session, we completed Lesson 1, and in this week's session, we'll complete Lesson 2.

- ***Say:***
  - In Lesson 2, we will focus on identification and evaluation of protection strategies for essential records.
  - We will begin by examining two strategies for handling risk: acceptance and mitigation.
  - Then we'll discuss various strategies for protection and storage of essential records.
  - Finally, we'll address planning for the availability of essential records and the issues that should be considered when evaluating protection strategies.

Transition: Let's take a look at the objectives for Module 2.

PG 3-8

Show slide 3-5.



Module 2 Objectives

Review the module objectives.

Point out that we covered the first objective in Session 2, and we'll be addressing the second objective in this session, as indicated with bold text.

Transition: Let's get started with Lesson 2 and talk about the strategies for handling risk.

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**

[This page intentionally left blank.]

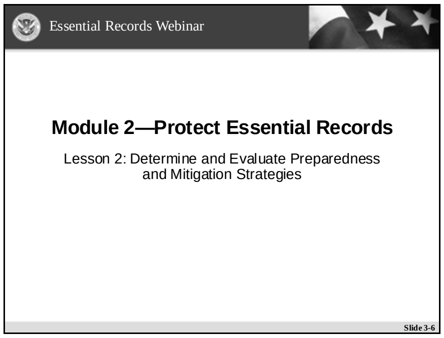
Lesson 2: Determine and Evaluate Preparedness and Mitigation Strategies

PG 3-9

(Duration: 30 minutes)

START TIME: ______________

Show slide 3-6.



Introduce the lesson.

Say:

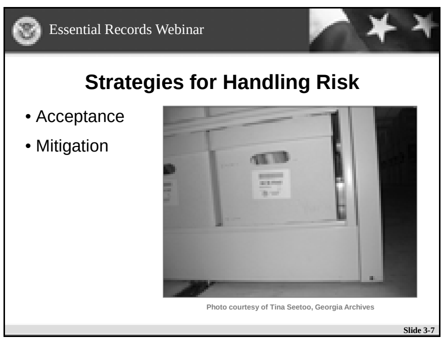
- Identification of critical business functions, selection of essential records, and assessment of risks are all important preparatory steps, but just having a list of essential records is not enough. You must also take steps to protect that essential information.

- This lesson will discuss different ways to protect your essential records.
- Let's start by taking a look at the three strategies for handling risk.

PG 3-10

Strategies for Handling Risk

Show slide 3-7.



Introduce the strategies for handling risk.

Say: You basically have two choices for handling potential risks to records. Either you accept the risk or your take action to mitigate the potential for damage.

Once you have identified and evaluated the risks to your essential records, you must decide how you want to handle those risks. Because handling risks involves costs (time, effort, and money), you will need to evaluate and select the best and most cost-effective strategies.

Your decision on how to handle the risks to your essential records is what drives the selection of your prevention or mitigation strategies.

There are basically two strategies for handling risk to essential records:

- Acceptance
- Mitigation

Say: Let's take a closer look at each of these strategies.

Acceptance

Review acceptance as a strategy for handling risk.

Acceptance involves recognition of the existence of a specific risk and acceptance of the impact of the risk, should it occur. No action is taken (i.e., the "do nothing" option).

For example, records storage is provided in the basement of your facility on pallets only. There is no other storage space available, and there are no funds to move the records to a safer environment. So, the records have to be stored in the basement; you have to accept the records storage risk.

Mitigation

Review the variety of approaches that can be taken to mitigate risk to records.

Mitigation involves taking steps to minimize the likelihood or impact of an emergency. You may not be able to prevent a risk or threat from occurring, but you may be able to reduce the likelihood of its occurrence, or mitigate the impact it has on your agency if it does occur.

For example, in the situation just described, you may accept the storage risk, but you have moved records from pallet storage to metal shelf storage at least 6" off the floor. You have now mitigated some of the risk to the records.

Point out how sound records management practices can provide a measure of security against potential threats.

Remind participants that the self-directed IPER course, *Introduction to Records and Information Management for State and Local Governments*, covers the basic concepts and principles of records management. They should also consult their agency records manager and/or the state archives and records management agency if they have questions about or need assistance in implementing a records management program.

Implementation of sound records management practices agency-wide provides a measure of security against potential threats. Records stored in boxes are more likely to survive a leaky roof or wind damage than records stored in loose stacks on open shelving. If records have been properly scheduled, you have a ready reference that can guide you in determining which records to "rescue" when the storage space is threatened, and determining which are near the end of their active life anyway and can be let go.

Explain how transfer of risk is another approach to mitigation. The use of records centers that are run by government agencies or private entities is a good example of this approach. Storage of security microfilm at the state archives is another example that is available in many states.

Another approach to mitigation involves transfer of the risk (in whole or in part) to another agency, individual, or entity: for example, storing your essential records at a records storage facility managed by another entity.

Most states operate records centers for storage of records from state agencies. A number of counties and cities also run record centers for agencies in their jurisdictions.

More than half of the state archives allow local governments to store microfilm copies of records in their vaults. On several occasions, counties and cities have been able to reconstruct essential records from this microfilm when the originals were destroyed in courthouse fires and similar events.

These strategies do not necessarily eliminate risk; they only transfer the impact. However, if the third party is more qualified than your agency to deal with the risk, transfer of the risk may also reduce it.

Tell participants if either a state-run record center or security microfilm storage is available in your state.

- If the records center is available, ***explain*** what records would be appropriate to transfer to it and whom to contact.
- If your state archives accept security microfilm from state or local agencies, ***explain*** how to access this service.
- If neither of these options is available in your state, ***provide*** alternatives if they are available—for instance, commercial storage facilities or cooperative agreements between two counties to store copies of each other's most essential records.

Other strategies for mitigating risk include:

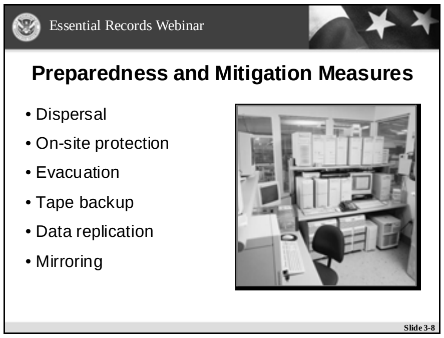
- Requiring passwords to increase security for electronic records
- Locking up records and establishing security protocols to prevent unauthorized access
- Maintaining good housekeeping to prevent fire or other damage to records

Transition: Let's look at some of the other specific actions you can take to protect your essential records.

PG 3-12

Preparedness and Mitigation Measures

Show slide 3-8.



Explain that some states or localities have guidelines and regulations regarding protection of essential records.

Tell participants to check the IPER Resource Center for additional information on their state.

Some states or localities have guidelines and regulations regarding protection of essential records. This varies widely from state to state. Check the Intergovernmental Preparedness for Essential Records (IPER) Resource Center for additional information on your state.

Explain that if there are no regulations in place, you have a choice on how to handle the risks:

- Accept the risks and do nothing.
- Mitigate the risks by protecting your records.

If there are no regulations in place for your state or locality, then you have a choice on how to handle your risks. If you choose to accept the risk, then you don't need to do anything else. But if you decide to mitigate risk and protect your records, then you'll need to determine your preparedness or mitigation measures.

Review the actions that you can take to protect records.

There are several actions you can take to protect your essential records, including:

- Dispersal
- On-site protection
- Evacuation
- Tape backup
- Data replication
- Mirroring

NOTE TO INSTRUCTOR:

You may be asked about e-vaulting, a protection action not discussed in this training. If someone does ask, ***refer*** participants to the e-vaulting information on the IPER Resource Center.

- URL: *http://www.statearchivists.org/resource-center*

Point out that making copies of records is one of the most effective ways to protect essential information.

Explain that when copies exist, we are often as concerned about safeguarding those copies of the records as we are about the safety of the original record.

Say: We'll discuss more about copying records shortly.

One of the most effective ways to protect the information contained in essential records is by making copies of those records. Therefore, we are often as concerned about safeguarding those copies of the records as we are about the safety of the original records themselves.

When making copies is not practical, we must, of course, work doubly hard to ensure that the original records are safeguarded.

From a legal point of view, it is also important to remember that copies of some records, if not certified or created in a systematic authoritative way, may not have the legal standing of the originals.

Say: Let's take a closer look at each of these measures.

Dispersal

Explain dispersal.

With dispersal, copies of essential records are distributed to other locations. There are two types of dispersal:

- Routine—Routine dispersal occurs during the regular course of business. You may find that you are already creating and protecting copies of essential records at different locations through your normal business processes. For example, a key document that is generated at your headquarters might also be sent to one or more field offices on a regular basis, or copies of essential documents (for example, birth records) may be sent to the state as part of regular office routine. Study your agency business processes to determine where, how, and when such information is shared.
- Planned—Planned dispersal involves the duplication and distribution of essential record copies that are created specifically for protection purposes. Computer system and network backup tapes of essential records that are stored off site are examples of copies made on a regular basis and stored somewhere else, solely for the purpose of Continuity of Operations (COOP) and disaster recovery.

Say:

- This is a good place to point out the importance of managing records that are kept on backup tapes.
- In an emergency you need to be able to locate and access essential records promptly without wading through backup tapes filled with non-essential, or even obsolete, records.

- Backups are important, but backing up everything—without isolating the essential records—is not a good solution.
- "Isolation" of essential records can take place physically (by placing them on separate backup tapes) or virtually (by indexing them in such a way that they can be located rapidly).

On-Site Protection

Explain on-site protection.

You may need to keep some essential records on site. For these records, you can use special equipment such as fire-resistant cabinets and vaults to protect the information. You can also plan secured storage rooms, but you have to develop specifics to meet the needs of the agency. You can also implement other measures—for example, storing records on metal shelves (wooden shelves absorb water) 6" or more off the ground.

Evacuation

Explain evacuation.

If the original essential record cannot be copied and cannot be protected on site, you may have to plan to collect the originals and transfer them to another site when an emergency occurs. With this protection method, you will have to plan exactly:

- What will be evacuated
- Where it will be evacuated
- How it will be evacuated
- How it will be stored, managed, and accessed in its new location
- When it will be evacuated

Point out that evacuation is common practice along the Gulf and Atlantic Coasts when hurricanes are approaching. Many counties load enormous quantities of irreplaceable records onto semi trucks and take them hundreds of miles inland.

Tape Backup

Review tape backup.

Tape backup can take from hours up to a day for recovery time (i.e., retrieving tapes from an off-site facility, physically getting them to the alternate site, loading them, accessing data, etc.). This method may be an option for information with longer recovery time objectives (RTO).

Explain RTO:

- ***Say:*** Recovery time objective, or RTO, is widely used in information technology (IT) when discussing business continuity and recovery. RTO defines how soon after an emergency a computer system, network, or application must be restored to functional status to minimize disruption of normal operations and loss of revenue.

Data Replication

Review data replication.

Data replication is used to replicate data at one or more sites, such as a primary processing site and an alternative site, so that the information is accessible in the event that the primary site becomes unavailable. Data replication is used when data must be continuously available or when data recovery must be accomplished in a very short period of time.

Mirroring

Review mirroring.

Mirroring is a method of data replication that maintains a replica of electronic records, such as those found in databases and/or file systems, by applying changes at the secondary site simultaneously with the changes at the primary site. Mirroring requires enough network bandwidth to transport data at sufficiently fast speeds to ensure that the process is successful.

Say: For more information on determining protective measures for electronic records, the NIST publication SP 800-34 is a helpful resource.

For more information on determining protective measures for electronic records, refer to *NIST Contingency Planning Guide for Information Systems*, publication SP 800-34 at: *http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1.pdf*

Point out that the URL to this web page is provided in the Participant Guide on page PG 3-14, as well as in the "References" section of **Reference 01**—Resource Center, References, Reading List.

- ***Remind*** participants that this document is available for download with their session materials.

Transition: Let's talk more about creating copies of essential records.

PG 3-15

Duplication of the Original Records

Show slide 3-9.

Duplication and Copying Formats

Review the various formats used to duplicate essential records.

Because one of the most effective ways to protect the information contained in essential records is to make copies of those records, it is important to understand the options available for making such copies.

There are several different formats you can use when creating backup copies of essential records. Your backup copies may be in a different format than the original record.

Duplication formats include:

- **Microform**—Documents can be filmed or output to microfilm or microfiche.
- **Digital formats**—You may choose to scan documents or download data and store them on computer media. While this format allows you to store a great deal of information in a small space and access it easily in the short run, you should also determine what software and hardware will be needed to access the data, the costs of reformatting the data, and the costs of maintaining access to data stored off site.

Say: For those of you who may already duplicate your data in digital formats, think about what format the information is in—MS-Word, text, JPEG, PDF, or something else? Some of these may not be open standards. You should investigate open standards—such as TIFF and XML—as a means to help ensure accessibility.

- **Backup tapes**—Computer backups created in the normal course of system maintenance, or other electronic copies that may be created routinely in the normal course of business, can be used as the essential record copies. However, remember that system backups may not be structured in a way that is most convenient for immediate access to the records. Be aware that retrieval of records to meet Freedom of Information requests or legal discovery may be cumbersome, especially if tapes are dispersed and sometimes "lost" in obscure locations. Courts may penalize agencies for not responding fully to requests in a timely manner. Work with your information technology (IT) staff to determine whether backup tapes represent an appropriate option for your particular circumstances and requirements. If the backup tapes' location is the same as your own location, determine whether this location is sufficiently distant from the site of risk to avoid the effects of the risk.

- **Paper—**Paper copies are typically the least expensive method of reformatting, but the most cumbersome to update and distribute—and they may also have associated costs for storage off-site, costs which depend on the quantity of records identified as essential records.

Explain that it's critical to ensure that all necessary information is transferred to the copy and that it be done in a standardized format.

Regardless of the format used, it is critical to ensure, when your information is duplicated, that all the necessary information is transferred to the copy and that the record can be readily accessed. Remember: Accessibility may depend on whether the data have been captured in a standard format.

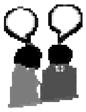
Say:

- The National Incident Management System (NIMS) points out in the fifth component of the system—the "Ongoing Management and Maintenance" component—that technical standards may need to be developed—and adopted by all levels of government—to ensure that information can be shared reliably across jurisdictions.
- NIMS is overseen and directed by the National Integration Center (NIC), part of the Department of Homeland Security, and NIC coordinates the establishment of technical standards for NIMS users.

Explain the evidential value of a copy.

The "evidential value" of the copy (the ability to be as authoritatively referenced as the original) must be maintained by having the copy well-documented. For fixed film images (microfilm, microfiche, photographic images) the following may be required:

- An unmanipulated image that has not been dodged, burned, retouched, tinted, or airbrushed, either in the darkroom or afterwards
- Documentation on when, where, how, why, and by whom the image was taken and what it documents
- A record of a continuous chain of custody by the creator (photographer or his or her employer)



Lead a group discussion:

- ***Say:*** It can be difficult to decide which format to use when making copies of records.
- ***Ask:*** Think about the essential records you have identified in your agency. What formats would you use to make copies of them?
- ***Tell*** participants to raise their hands to answer or to type their answers in the Chat tool, using the "Public" tab.
- ***Call on*** participants who have their hands raised.
  - ***Remind*** participants to take their phones off mute before speaking.
- ***Acknowledge*** any responses provided in the Chat tool.
- ***Confirm or correct*** responses as appropriate.
  - **Expected answers:** will vary
- If no participants respond, ***provide*** the following examples:
  - Older minutes and case files—microfilm and send copy to state archives or another storage facility for security storage

  - Blueprints and engineering diagrams for existing buildings or utilities—scan and store electronically in two or more locations

Ask:

- In your agency, how do you currently back up essential records that are typically created and stored on computers (e.g., recent minutes, payrolls, voter registrations)?
- Do you have the software and hardware needed to access these files?
- Are they in a format that can be read immediately?

Say: It's important to point out that simply backing up or copying records does not equal effective records management.

Retention of Backup Copies

Review retention of backup copies.

The backup copy of the essential record stored off site is normally a duplicate of the original record. You will want to designate which is the original record and which the copy.

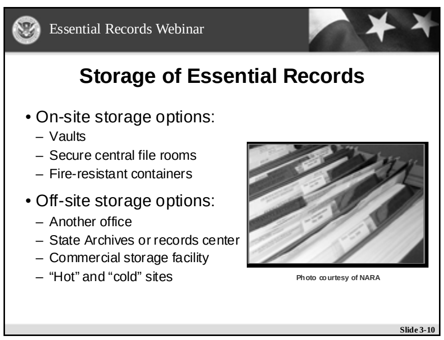
The original essential record must be retained for the period specified in your agency's records retention schedule. Typically, the essential record copy is destroyed or deleted when it is replaced by an updated copy of the original essential record.

Transition: After you have decided how to protect your essential records, you will need to determine where to store them.

Storage of Essential Records

PG 3-17

Show slide 3-10.



Explain that agencies have two options when selecting storage methods for their essential records: on site or off site.

Agencies have two options when selecting storage methods for their original essential records: on site or off site. Whichever you choose, be sure to check the laws and regulations for the storage of government records in your state or locality. Some states prohibit the transport of official records across state lines, so under those circumstances records cannot be sent to an off-site storage facility in another state.

On-Site Storage

Sometimes keeping your essential records off-site is not an option; you need to keep them on the premises, at or near the point of creation.

Review the on-site storage options.

On-Site Storage Options

Some options for on-site storage include:

- Vaults
- Secure central file rooms
- Fire-resistant containers

Point out that a fire-resistant safe may not protect magnetic, electronic, or optical media, and fire-resistant storage may not protect against charring or combustion when the safe is opened.

Say: If your on-site essential records volume is particularly large, you may even establish an essential records building.

If the volume of your essential records is particularly large, and if your holdings are all in one location, you may even establish an essential records building. This building must meet all your state or local standards for the proper storage and protection of records and the information they contain.

Say:

- Most states have regulations for the storage of government records that address issues like security and climate control; some have regulations concerning location (for example, records may not be stored out of state).
- We have heard about several cases in which records destroyed in courthouse fires or by hurricanes have been reconstructed from security microfilm deposited at the state archives.

Off-Site Storage

Explain that the location of the off-site storage facility affects access to records during an emergency.

Point out that we'll be talking about access to essential records in greater detail in Session 4.

The choice of an off-site storage facility will play an important part in the availability of your essential records should an emergency occur.

Explain that the off-site facility should be close, but not too close.

Say:

- Off-site storage should be a minimum of 30 miles away from the site of the original records.
- In those areas that are subject to widespread emergencies, however, it may be wise to store copies of essential records much farther away—from hundreds of miles to more than a thousand.
- You will need to make sure that authorized personnel have access to the remotely stored records in case local staff cannot travel to the remote site.

The off-site storage facility you choose should be sufficiently remote from the location of the original records that it would not be subject to the same emergency, but close enough to allow ready retrieval. Based on your agency's risk assessment and analysis, you will need to determine the appropriate distance away from your facility that will protect your agency's essential records adequately.

Point out that off-site protection almost certainly requires duplication of essential records.

Whereas on-site protection may or may not involve duplication, off-site protection almost certainly will.

Review the off-site storage options.

Off-Site Storage Options

Some of the options for off-site storage are:

- Off site at another office:
  - If your agency has offices in other locations, you may be able to use them to store copies of your essential records.
  - If your agency has a working relationship with another agency or agencies, you may reach reciprocal agreements to store each other's essential records.
- Off site at the state archives or records center:
  - Security microfilm: More than half of the state archives and records management programs offer storage for security microfilm from state and local governments. In several states, important records destroyed in courthouse fires or by hurricanes have been reconstructed from security microfilm deposited at the state archives.
  - Paper-based records: Most states provide records centers for the storage of temporary (largely paper-based) records from state agencies; this could include essential records protection. A few offer similar services to local governments, while some cities and counties operate their own records centers.
- Off site in a commercial storage facility:
  - Numerous vendors provide storage and services for essential records. You must ensure that their facilities meet all the state or local standards for the protection of records.

NOTE TO INSTRUCTOR:

- ***Be prepared to describe*** the availability of records storage services for state and local governments in your jurisdiction. If your state has specific storage regulations that apply to essential records, you could share them with participants at this point and/or show participants the IPER Resource Center's section on Storage.
- URL: *http://www.statearchivists.org/resource-center*

Review hot and cold sites.

Hot Sites and Cold Sites

Off-site storage facilities can go beyond just storage. They can also serve as "hot" sites or "cold" sites:

- A "hot" site includes everything you need to continue operations: computers, phones, fax machines, copiers, scanners, office supplies, etc., allowing you to go to the hot site, sit down, and work.
- A "cold" site provides space for you to bring in whatever equipment you need, but does not provide the equipment, supplies, etc., you need to continue operations. Cold sites are less expensive than hot sites and take longer to become operational.

Point out that there is also an option of a "warm" site, which has connectivity and is operational, but on a smaller scale than a hot site (which duplicates the operation and often has real-time data exchange).

Say: If your agency does choose to use off-site storage, there are some important factors you should consider.

Review the considerations for off-site storage.

Considerations for Off-Site Storage

It is important to remember the following when choosing an off-site facility in which to store essential records:

- Equipment and electricity may be needed to access the records.
- The facility should have 24-hour security and be environmentally controlled for temperature and humidity.
- The facility should allow 24-hour access by appropriate agency officials.
- The facility should be inspected for water leaks along walls and floors and around windows.
- The facility should have fire suppression and/or smoke detection systems that are connected to local emergency officials.
- Cost of storage may depend on the volume of essential records and the storage format.
- Alternative locations under consideration as hot sites should be on a separate electrical grid from the home site or have a back-up generator.

NOTES TO INSTRUCTOR:

- ***Go to*** the IPER Resource Center as directed below, only if your audience's state has regulations or guidelines addressing the protection of records.

- If no such guidelines exist, either ***show*** an example from another state, such as the Oregon State example below, or ***skip*** this step.
  - An example from the Oregon State Administrative Rules is found at *http://www.arcweb.sos.state.or.us/rules/OARS_100/OAR_166/166_020.html*
    - Records storage standards are found in 166-020-0015 on that page.
    - Requirements for essential records are found in 166-020-0045 on that page.

Say:

- You can find links to your state's regulations or guidelines addressing the protection of records on the IPER Resource Center.

- Let's take a moment to visit the Resource Center and look at these guidelines.

Launch web page in iLinc:

- Web page: IPER Resource Center
  - URL: *http://www.statearchivists.org/resource-center*
- ***Access*** the page for your state.
- ***Point out*** the regulations or guidelines addressing the protection of records.

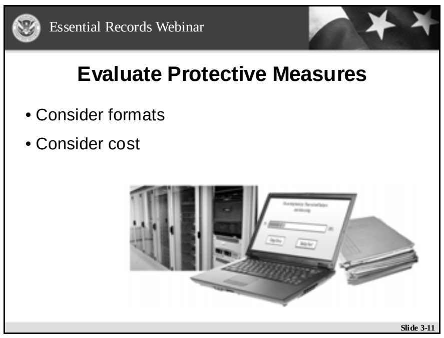
When done, ***close*** the web page for everybody by selecting “Close All” when prompted.

Transition: Now let’s focus on evaluating protective measures and take a look at the factors that need to be considered when determining which protective measure to use.

PG 3-20

Evaluate Protective Measures

Show slide 3-11.



Consider Formats

Review how to consider format when determining a protective measure.

As you explore protective measures, you need to consider special media needs. For example, paper, photographs, microforms, and electronic media all have specific storage condition requirements, and all have different characteristics that must be addressed when they are wet or damaged. You must consider provisions for each medium in your plan of action for handling risk.

You must protect essential records using the method that best suits the record’s medium, the record’s cycle of updates, and the need for immediate accessibility. The protection strategy you apply must include decisions about what medium or media you will use to store your essential record. Remember, your essential record is not necessarily in the same medium or format as the original.

Review the questions to ask when determining a protection strategy, with regard to the media requirements of the specific essential record.

Answering the following questions will help you to determine your protective measures with regard to the media requirements of the specific essential record:

- Is the information in the record static? Would a paper copy suffice?
- Is the information in the record dynamic?
- What is the timeframe for recovery?
- Do several employees need copies of the document—i.e., phone tree, file plans, etc.?
- What is the volume involved?
- Is the original format critical to its function (e.g., audio to transcript)?
- Will a change in format involve a loss of information (e.g., metadata)?

Open a document from the “Course Handouts and References” WebSync file in iLinc.

- Document name: **Handout 3.1**—Protection Strategies Based on Media Requirements
- ***Refer*** participants to **Handout 3.1**—Protection Strategies Based on Media Requirements for answers to these questions.
- ***Review*** the handout and explain the information provided in each table.

When done, ***close*** the document for everybody by selecting “Close All” when prompted.

Refer to **Handout 3.1**—Protection Strategies Based on Media Requirements for answers to these questions.

NOTE: Electronic copies of fixed format (paper, microfilm or microfiche, photos) records created as “backups” or for off-site access should NOT be considered appropriate for long-term preservation unless they have been created to archival standards. These records may become inaccessible without special attention.

Consider Cost

Review how cost should be considered when determining a protective measure.

The cost of protecting essential records will require a long-term commitment from management. Management must be able to weigh the cost of protecting the records against the risk of not recovering the records in the event of an emergency or disaster.

You could undertake a cost-benefit analysis in order to identify the most cost-effective way to protect the essential records and to resume business in a determinate amount of time. Whether you do this as a formal cost-benefit analysis or not, try to look for cost-effective ways to protect records and use risk assessment to determine how quickly essential records are needed.

Ask: Before moving on, are there any questions about what we've covered so far?

Resolve any outstanding questions.

Transition: Let's review what we covered in this session. Then we'll do an activity to apply what we've learned. And to complete the module, we'll go over your Take-Home Activity.

Session 3 Review and Wrap-Up

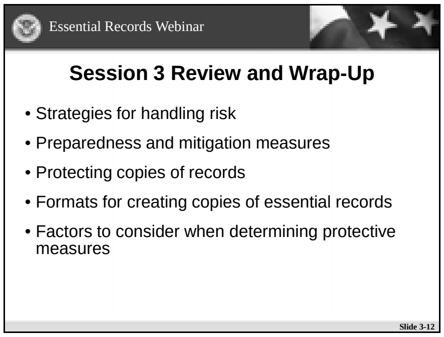
Session Review

PG 3-23

(Duration: 5 minutes)

START TIME: ______________

Show slide 3-12.



Review the key points covered in this session.

Say: In this session, we took a look at protecting your essential records.

NOTE TO INSTRUCTOR:

- The Session Review can be conducted as a question and answer (Q&A) session or as an instructor presentation. Instructions are provided below for each approach.

Q&A instructions:

If time allows, *facilitate* the review by turning some or all of the bullet points into questions.

- For example:
  - ***Ask:*** Who can tell me the strategies for handling risk? Answer via the Chat tool, using the "Public" tab.

Open a prepared Powerboard in iLinc:

- **PB 3.1**—Session 3 Review
- ***Review*** the key points covered in this session, as provided on the Powerboard.
- ***Turn*** the bullet points into questions, as appropriate.
- As participants answer the questions, ***type*** the correct answers on the Powerboard, under the appropriate bullet.
- ***Use*** the notes from the instructor presentation section to help formulate your questions and for the correct answers.

When you are done with the review, ***close*** the Powerboard for everybody by selecting “Close All” when prompted.

- ***Do not save*** the Powerboard.

Instructor presentation review instructions:

Review the key points covered in this session, as provided on the slide.

Elaborate on the bullet points as follows.

- NOTE: For each bullet point, you may opt to redisplay the relevant slide to help reinforce retention. Slide references are provided.

- Strategies for handling risk
  - OPTIONAL: Redisplay slide 3-7, "Strategies for Handling Risks"
  - ***Say:*** We started with two strategies for handling risk:
    - Acceptance
    - Mitigation
- Preparedness and mitigation measures
  - OPTIONAL: Redisplay slide 3-8, "Preparedness and Mitigation Measures"
  - ***Say:*** Then we looked at the preparedness and mitigation measures available to protect your essential records:
    - Automatic or routine dispersal
    - Planned dispersal
    - On-site protection
    - Evacuation
    - Tape backup
    - Data replication
    - Mirroring

In Session 3, you learned:

- Strategies for handling risk
- Preparedness and mitigation measures

- Protecting copies of records
  - OPTIONAL: Redisplay slide 3-9, “Duplication of the Original Records”
  - ***Say:*** We learned that one of the most effective ways to protect the information contained in essential records is to make copies of those records; therefore, we are often as concerned about safeguarding those copies as we are about the safety of the original records themselves.

- Protecting copies of records

- Formats for creating copies of essential records
  - OPTIONAL: Redisplay slide 3-9, “Duplication of the Original Records”
  - ***Say:*** There are several different formats you can use when creating copies of essential records:
    - Microform
    - Digital formats
    - Backup tapes
    - Paper

- Formats for creating copies of essential records

- Factors to consider when determining protective measures
  - OPTIONAL: Redisplay slide 3-11, “Evaluate Protective Measures”
  - ***Say:*** Finally, we took a look at the factors we need to consider when determining which protective measure to use:
    - Format
    - Cost

- Factors to consider when determining protective measures

Ask: Are there any questions before we begin the activity?

Resolve any outstanding questions.

Transition: Let's practice what we have learned today.

Activity: Determine Protection Strategies and Measures

PG 3-24

(Duration: 25 minutes)

START TIME: ______________

Show slide 3-13.

Introduce the activity.

Facilitate the activity using the Activity Instructions on page IG 3-57.

Activity materials:

- **Handout 1.6**—The Division of Public Recreation (DPR) Overview
- **Handout 2.3**—Identify and Evaluate Risks Activity
- **Handout 3.2**—Determine Protection Strategies and Measures Activity

[This page intentionally left blank.]

Activity Setup

Activity Snapshot:

Activity Name:	Determine Protection Strategies and Measures
Activity Purpose/Goal:	Practice determining a strategy for handling risk (acceptance or mitigation) and selecting the appropriate prevention or mitigation measure for that strategy.
Notes:	This is a two-part activity: • Part 1 is to be completed during the webinar session. Using the DPR risks identified in the Session 2 activity, participants are asked to (1) select a strategy for handling each risk and (2) determine the appropriate protective measure(s) for each risk. • Part 2 is to be completed as a Take-Home Activity, outside of the webinar session. Using their respective agencies' essential records and identified risks from the Session 2 activity, participants are tasked with (1) selecting a strategy for handling each risk and (2) determining the appropriate protective measure(s) for each risk.
Prerequisite for Subsequent Activities (name and location of subsequent activities):	• Session 4 Activity: Determine Timeframes for Accessibility on page IG 4-41 of the Instructor Guide and page PG 4-23 of the Participant Guide.
Group or Individual Activity:	• Part 1 is an individual activity. • Part 2 is an individual activity. NOTE: Depending upon the make-up of the class, this activity can also be a group activity performed by teams from the same agency.
Time to Complete Activity:	• Part 1 = **20 minutes** total: – **5 minutes** for introduction – **10 minutes** for participant work time – **5 minutes** for debrief • Part 2 = **5 minutes** total: – **5 minutes** for Take-Home Activity introduction

Required Materials (name and location):	• Part 1: – **Handout 1.6**—The Division of Public Recreation (DPR) Overview – **Handout 3.2**—Determine Protection Strategies and Measures Activity • Part 2: – **Handout 2.3**—Identify and Evaluate Risks Activity – **Handout 3.2**—Determine Protection Strategies and Measures Activity
Activity Scenario (if applicable):	• Part 1: – Participants are tasked with selecting strategies for handling risks and determining appropriate protective measures for a fictitious agency’s essential records. • Part 2: – N/A
Activity Debrief:	• Part 1: – Group discussion • Part 2: – Group discussion, conducted at the beginning of Session 4

Activity Instructions

Instructions:

Tell participants to locate the materials for the activity:

- **Handout 1.6**—The Division of Public Recreation (DPR) Overview
- **Handout 2.3**—Identify and Evaluate Risks Activity
- **Handout 3.2**—Determine Protection Strategies and Measures Activity

Tell participants to raise their hands when they've located all the documents needed for the activity.

- ***Assist*** any participants having trouble locating the necessary documents.

Say: The purpose of this activity is to practice determining a strategy for handling risk (acceptance or mitigation) and selecting the appropriate prevention or mitigation measure for that strategy.

Tell the participants that this is a two-part activity:

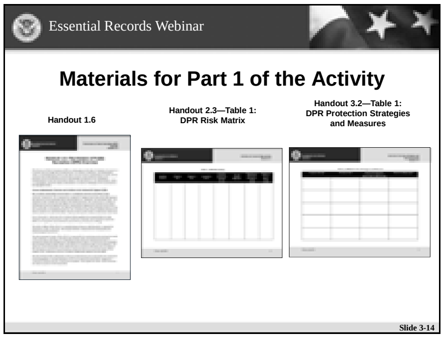
- Part 1 is to be completed during the webinar session.
- Part 2 is to be completed as a Take-Home Activity outside of the webinar session.

Begin Part 1 of the activity.

Say: In Part 1, using the Division of Public Recreation risks you identified in the Session 2 activity, you will (1) select a strategy for handling each risk and (2) determine the appropriate protective measure(s) for each risk.

Say: Let's take a look at the materials you'll be using for Part 1.

Show slide 3-14.



Continued on next page...

Tell participants to go to **Handout 1.6**.

- ***Explain*** this is where they will find the information about the Division of Public Recreation.
- ***Explain*** that they may refer to this handout if necessary.

Tell participants to go to **Handout 2.3**, the DPR Risk Matrix table (Table 1).

- ***Explain*** this is where they will find the DPR essential record and related risks they identified in the Session 2 activity.

Tell participants to go to **Handout 3.2**.

- ***Point out*** the instructions for Part 1 on page 1 of the handout.
- ***Point out*** the DPR Protection Strategies and Measures table (Table 1), located on pages 3-4 of the handout.
- ***Explain*** that this is the table they will complete for the activity.

Say: Using the essential record and related risks identified in the Session 2 Activity (see the DPR Risk Matrix table on page 2 of **Handout 2.3**), complete the DPR Protection Strategies and Measures table by doing the following:

- In the **Essential Record** column, enter the essential record you used in the Session 2 activity.
- In the **Potential Risk** column, enter each risk to the essential record you identified in the Session 2 activity.
- In the **Protection Strategy** column, identify which protection strategy you will use for each risk. For example, essential records stored in a basement are at risk for water damage due to flooding. You decide you want to take measures to lessen this risk, so you decide on a mitigation strategy.
- In the **Protective Measures** column, describe the protective measures you will take to protect the essential record from the risks. For example, to mitigate the risk of a flood damaging your essential records, you may opt to perform on-site protection, such as storing the records at least 6" above the ground.

Continued on next page...

Tell participants to be prepared to share their answers with the class.

Tell participants they have **10 minutes** to complete the activity and fill in as many columns of information as they can.

Set up the Feedback tool in iLinc.

- ***Select*** the "Assignment status" answer set.

Tell participants to select "Completed" in the Feedback area when they have completed the activity.

Tell participants that you are going to remain silent so they can concentrate on the activity, and if they need to communicate with an instructor during the activity, to please do so via the Chat tool.

Tell participants to begin working.

Pause the iLinc recorder.

Monitor the activity:

- **Five minutes** into the activity, ***send a message*** to the class using the "Public" tab of the Chat tool.
  - ***Ask*** participants if they're doing OK or if anybody needs help.
  - ***Tell*** participants to raise their hand if they need help.
- ***Provide*** assistance as needed, using the "Private" tab of the Chat tool.

When **8 minutes** have passed, ***advise*** participants that they have **2 minutes** left for the activity.

When **10 minutes** have passed, ***tell*** the participants to stop working.

Restart the iLinc recorder.

Reconvene the class.

Debrief the activity using a large-group discussion:

Continued on next page...

Say: I need a volunteer to share an essential record, a risk to that record, and the protection strategy and measure you identified.

- ***Tell*** participants to raise their hands to answer or to type their answers in the Chat tool, using the “Public” tab.
- ***Call on*** participants who have their hands raised.
  - ***Remind*** participants to take their phones off mute before speaking.
- ***Acknowledge*** any responses provided in the Chat tool.

Confirm or correct responses as appropriate.

- Suggested answers are provided in bold in the Answer Sheet—DPR Protection Strategies and Measures Activity—Part 1 on page IG 3-63.
  - NOTE: The correct answers appear only in the IGs. The corresponding version of the table that is provided for the participants’ use does not contain the answers.
- ***Explain*** any correct answers that differ from the answer given by the participants.

For the non-presenting instructor: ***Open*** a new Powerboard and ***record*** the correct answers on the Powerboard.

Tell participants that they are welcome to record the correct answers in the DPR Protection Strategies and Measures table in **Handout 3.2**, but that they will also be receiving an email with the correct answers following the session.

Continue to debrief the activity until several participant responses have been addressed and all the answers provided in the DPR Protection Strategies and Measures table have been addressed.

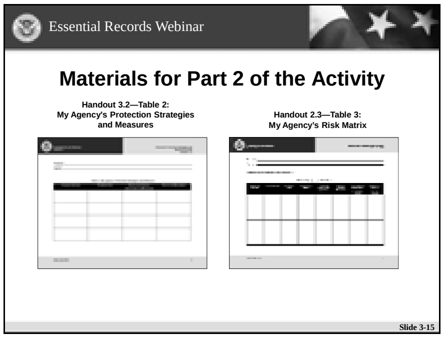
Ask for and resolve any questions.

Continued on next page...

Begin Part 2 of the activity.

Say: Let's take a look at the materials you'll be using for Part 2.

Show slide 3-15.



Tell participants to remain in **Handout 3.2**—Determine Protection Strategies and Measures Activity:

- ***Point out*** the instructions for Part 2 on page 5 of the handout.
- ***Point out*** the My Agency's Protection Strategies and Measures table (Table 2), located on pages 7-8 of the handout.
  - ***Explain*** that this is the table they will complete for the activity.

Say: For the take-home portion of this activity, you will be determining protection strategies and measures for identified risks, as you just did with DPR, except this time you will be doing it for your own agency. Using the two essential records and related risks for your agency you identified on **Handout 2.3** (the Session 2 activity handout), complete the My Agency's Protection Strategies and Measures table by determining a protection strategy and prevention or mitigation measure for each risk.

Tell participants that if they are taking this course with other folks from their agency, they can opt to work together and do this activity as a team.

Say: As part of your course materials, the My Agency's Protection Strategies and Measures table is provided as a Word document so you can complete it electronically and submit it via email.

Continued on next page...

NOTE TO INSTRUCTOR:

- ***Determine*** ahead of time to whom the participants should send their homework: Instructor 1 or Instructor 2.

Tell the participants to complete the assignment and email their completed sheets to <name of instructor who will receive the completed homework> no later than one day before the next webinar session (Session 4).

- ***Type*** the name and email address of the instructor to receive the homework in the Chat tool, using the "Public" tab.

Remind participants that they must complete all homework assignments in order to receive their Certificate of Completion.

Tell the participants to be prepared to share their answers with the class at the beginning of Session 4.

Tell the participants to keep **Handout 3.2** handy, as they'll need them it Session 4.

Ask for and resolve any questions.

End the activity.

Answer Sheet—DPR Protection Strategies and Measures Activity—Part 1

Table 2: DPR Protection Strategies and Measures

Essential Record	Potential Risk	Protection Strategy (Acceptance or Mitigation)	Protective Measure(s)
System Backup Tapes	Lack of Climate Control—Flooding	Mitigation	Dispersal—Send backup tapes to off-site storage—Rotate weekly
Open Contracts in Basement	Lack of Climate Control—Flooding, wet records, and the growth of mold and mildew	Mitigation	Move records to storage facility
Current Public Comments	Lack of Climate Control—Flooding, wet records, and the growth of mold and mildew	Acceptance	Leave files in place and accept risk that they may be damaged
EEO Files in Basement	Lack of Climate Control—Flooding, wet records, and the growth of mold and mildew	Mitigation	To prevent water damage in case of flooding, move records off bottom shelf until a secure storage facility can be obtained
Server in Basement	Lack of Climate Control—Flooding, temperature and humidity controls, damage to the system	Mitigation	Build and move server to an environmentally controlled space on a higher floor

[This page intentionally left blank.]

Show slide 3-16.

Remind participants that they can access course materials, as well as contact instructors and IPER staff, through their own Participant Dashboard on the IPER Resource Center.

Say: This concludes Session 3 of the *Essential Records Webinar*.

Say: Next week, in Session 4, we'll talk about ensuring access to your essential records during an emergency and incorporating your essential records into COOP Plans. We'll meet on <date of Session 4> at <time of Session 4>.

Ask for and resolve any outstanding questions.

Say: Please don't hesitate to contact us, should you have any questions about the content we covered today or about the Take-Home Activity. Our names and contact information are provided in the Chat tool.

- ***Type*** your names and contact information in the Chat tool, using the “Public” tab.

Say: We’d like to remind you that you’re welcome to send us an email and let us know your thoughts on the course thus far, and let us know if there’s anything that we can do to improve the course or your experience.

Stop the iLinc recorder.

End the webinar session.

- ***Remember*** to dismiss all the participants in iLinc.

NOTE TO INSTRUCTORS:

Immediately after the conclusion of Session 3, ***do the following:***

- ***Email*** the answer sheet to Part 1 of the Determine Protection Strategies and Measures activity to the participants.