



# Essential Records Webinar

## Session 3

Participant Guide  
*Final, July 2010*



FEMA

Course Number: AWR-210-2





## Table of Contents

**Session 3 Introduction..... 3-1**  
    Session 3 Welcome and Overview ..... 3-1

**Take-Home Activity Debrief.....3-3**  
    Session 2 Activity: Identify and Evaluate Risk—Part 2..... 3-3

**Module 2— Protect Essential Records..... 3-5**

**Module 2 Introduction and Objectives ..... 3-7**  
    Module 2 Introduction ..... 3-7  
    Module 2 Objectives ..... 3-8

**Lesson 2: Determine and Evaluate Preparedness and Mitigation Strategies ..... 3-9**  
    Strategies for Handling Risk..... 3-10  
        Acceptance..... 3-10  
        Mitigation..... 3-11  
    Preparedness and Mitigation Measures ..... 3-12  
        Dispersal ..... 3-13  
        On-Site Protection..... 3-13  
        Evacuation..... 3-13  
        Tape Backup ..... 3-14  
        Data Replication..... 3-14  
        Mirroring..... 3-14  
    Duplication of the Original Records ..... 3-15  
        Duplication and Copying Formats ..... 3-15  
        Retention of Backup Copies ..... 3-16  
    Storage of Essential Records ..... 3-17  
        On-Site Storage..... 3-17  
        Off-Site Storage ..... 3-18  
    Evaluate Protective Measures ..... 3-20  
        Consider Formats ..... 3-20  
        Consider Cost..... 3-21

**Session 3 Review and Wrap-Up ..... 3-23**  
    Session Review ..... 3-23  
    Activity: Determine Protection Strategies and Measures ..... 3-24

[This page intentionally left blank.]



## Session 3 Introduction

### Session 3 Welcome and Overview

Slide 3-1

**Essential Records Webinar**  
Session 3

*Please stand by! The webinar will begin shortly.*

- 1** Join the conference call by dialing the conference number in your Invitation or Reminder Emails. Please put your phone on mute.
- 2** Be sure to have all Session 3 materials ready before the session starts. You'll find the link to the materials in your Invitation or Reminder Emails.

 **FEMA** | Course Number: AWR-210-2 Final, July 2010

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



Slide 3-2

Essential Records Webinar

### Session 3 Overview

- Take-Home Activity Debrief
- Module 2—Protect Essential Records
  - Lesson 2: Determine and Evaluate Preparedness and Mitigation Strategies

Slide 3-2



# Take-Home Activity Debrief

## Session 2 Activity: Identify and Evaluate Risk—Part 2

Slide 3-3

Essential Records Webinar

### Take-Home Activity Debrief

- Activity: Identify and Evaluate Risk—Part 2

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

Category of Risk	Priority	Impact of Risk	Frequency of Occurrence	Severity of Consequences	Current Controls	Residual Risk

Slide 3-3



[This page intentionally left blank.]



# Module 2— Protect Essential Records



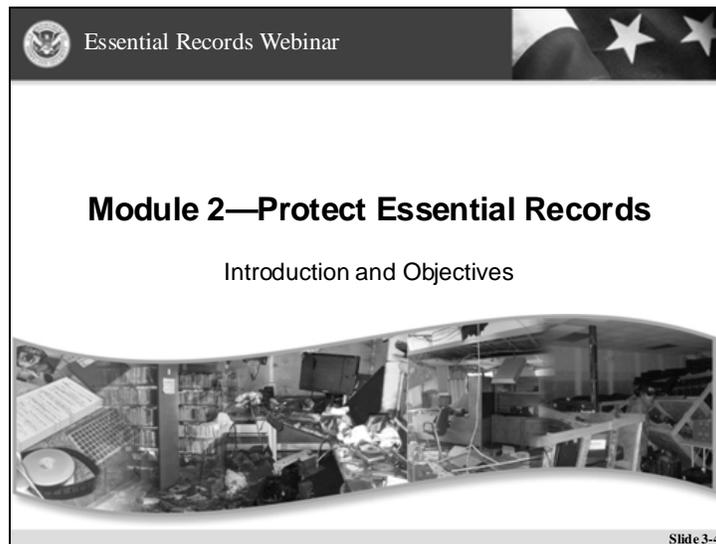
[This page intentionally left blank.]



## Module 2 Introduction and Objectives

### Module 2 Introduction

Slide 3-4





## Module 2 Objectives

Slide 3-5

Essential Records Webinar

### 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**

Slide 3-5

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 2: Determine and Evaluate Preparedness and Mitigation Strategies

Slide 3-6

The screenshot shows a presentation slide with a dark header bar. On the left of the header is the U.S. Department of Homeland Security logo, and on the right is a portion of the American flag. The main content of the slide is centered and reads: **Module 2—Protect Essential Records**  
Lesson 2: Determine and Evaluate Preparedness  
and Mitigation Strategies. In the bottom right corner of the slide, the text 'Slide 3-6' is visible.



## Strategies for Handling Risk

Slide 3-7

Essential Records Webinar

### Strategies for Handling Risk

- Acceptance
- Mitigation

Photo courtesy of Tina Seetoo, Georgia Archives

Slide 3-7

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

### Acceptance

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

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.

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.

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.

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



## Preparedness and Mitigation Measures

Slide 3-8

Essential Records Webinar

### Preparedness and Mitigation Measures

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

Slide 3-8

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.

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.

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

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

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.

## 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.

## 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

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



## 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).

## 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

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.

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>



## Duplication of the Original Records

Slide 3-9

Essential Records Webinar

### Duplication of the Original Records

Duplication formats:

- Microform
- Digital formats
- Backup tapes
- Paper

Slide 3-9

### Duplication and Copying Formats

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.



- **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.

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.

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)

### 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.



## Storage of Essential Records

Slide 3-10

Essential Records Webinar

### Storage of Essential Records

- On-site storage options:
  - Vaults
  - Secure central file rooms
  - Fire-resistant containers
- Off-site storage options:
  - Another office
  - State Archives or records center
  - Commercial storage facility
  - “Hot” and “cold” sites

Photo courtesy of NARA

Slide 3-10

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.

#### *On-Site Storage Options*

Some options for on-site storage include:

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

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.



## Off-Site Storage

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

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.

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

### *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.



### *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.

### *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.



## Evaluate Protective Measures

Slide 3-11

Essential Records Webinar

### Evaluate Protective Measures

- Consider formats
- Consider cost

Slide 3-11

### Consider Formats

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.

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)?

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

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.



[This page intentionally left blank.]



## Session 3 Review and Wrap-Up

### Session Review

Slide 3-12

Essential Records Webinar

### Session 3 Review and Wrap-Up

- Strategies for handling risk
- Preparedness and mitigation measures
- Protecting copies of records
- Formats for creating copies of essential records
- Factors to consider when determining protective measures

Slide 3-12

In Session 3, you learned:

- Strategies for handling risk
- Preparedness and mitigation measures
- Protecting copies of records
- Formats for creating copies of essential records
- Factors to consider when determining protective measures



## Activity: Determine Protection Strategies and Measures

Slide 3-13

Essential Records Webinar

### Activity

- Determine Protection Strategies and Measures

Slide 3-13

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



Slide 3-14

Essential Records Webinar

### Materials for Part 1 of the Activity

Handout 1.6

Handout 2.3—Table 1:  
DPR Risk Matrix

Handout 3.2—Table 1:  
DPR Protection Strategies  
and Measures

Slide 3-14

Slide 3-15

Essential Records Webinar

### Materials for Part 2 of the Activity

Handout 3.2—Table 2:  
My Agency's Protection Strategies  
and Measures

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

Slide 3-15



Slide 3-16



**Thank You!**



**IPER**  
INTERGOVERNMENTAL  
PREPAREDNESS FOR  
ESSENTIAL RECORDS



**CoSA**  
Council of State Archivists



**FEMA**