Georgia Archives Essential Records Course

Session 1

Participant Guide

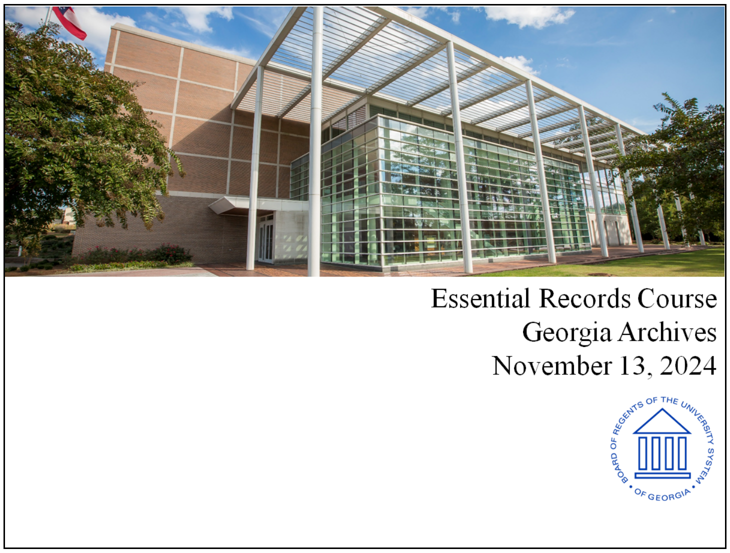
2024

Table of Contents

Course Introduction

Welcome to the *Essential Records Course*

Slide 1-1



Essential Records Course
Georgia Archives
November 13, 2024

Required materials for Session 1:

- Session 1 Participant Guide
- Session 1 Handouts
  - **Handout 1.1**—Essential Records
  - **Handout 1.2**—NIMS Resource Management Concepts and Principles
  - **Handout 1.3**—Potential Candidates for Essential Records Status
  - **Handout 1.4**—Examples of Information/Records, by Function, That Might Be Designated as Essential
  - **Handout 1.5**—Essential Records Questionnaire
  - **Handout 1.6**—Determine Essential Functions and Identify Essential Records Activity
- Course References:
  - **Reference 01**—Resource Center, References, Reading List
  - **Reference 02**—Key Terms for the IPER Courses

Contacts

Christine Garrett
Manager of Records Management
Christine.Garrett@usg.edu

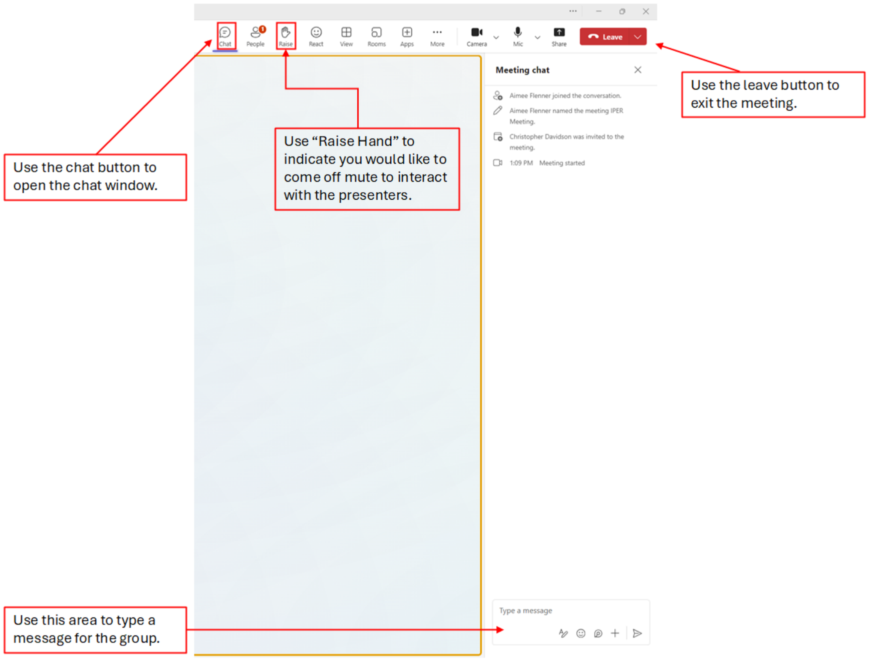
James Irby
Digital Preservation Technician
Sidney.Irby@usg.edu

Rebecca Wood
Records Manager
Rebecca.Wood@usg.edu

Sigourney Stanford
Conservator
Sigourney.Stanford@usg.edu

Christopher M. Davidson, J.D.
Associate Vice Chancellor, State Archivist
Christopher.Davidson@usg.edu

Slide 1-4



Aimee Flenner joined the conversation.

Aimee Flenner named the meeting IPER Meeting.

Christopher Davidson was invited to the meeting.

1:09 PM Meeting started

Use the chat button to open the chat window.

Use “Raise Hand” to indicate you would like to come off mute to interact with the presenters.

Use the leave button to exit the meeting.

Use this area to type a message for the group.

Slide 1-6

INTERGOVERNMENTAL PREPAREDNESS FOR ESSENTIAL RECORDS (IPER)

Program developed by the

COUNCIL OF STATE ARCHIVISTS (CoSA)

In cooperation with the

NATIONAL ARCHIVES & RECORDS ADMINISTRATION (NARA)

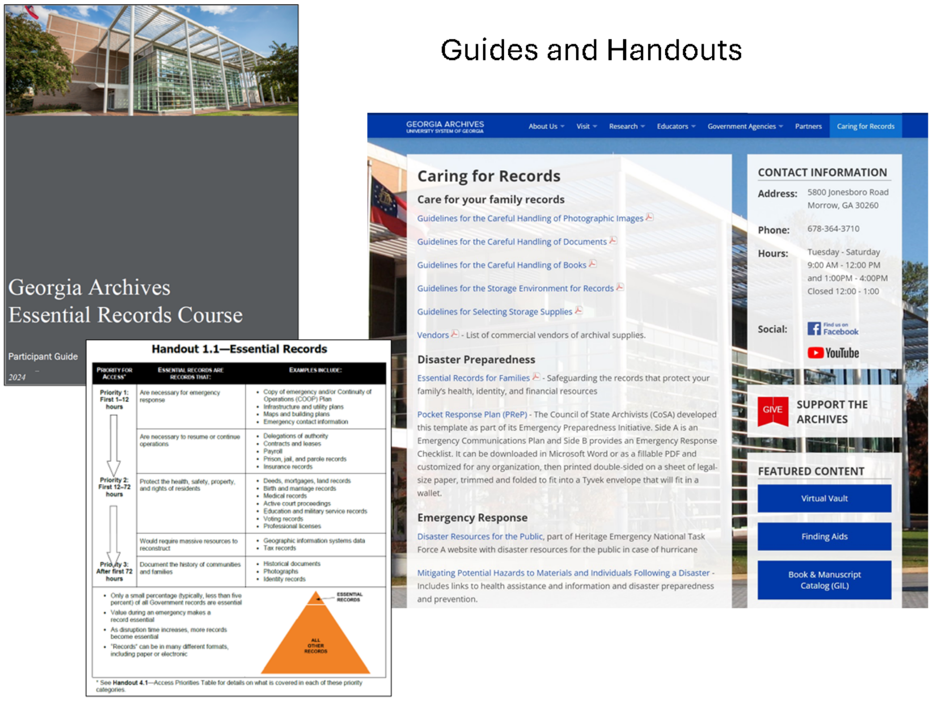
And sponsored by the

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

Archives Website and the Participant Guide

Slide 1-7

Guides and Handouts



Georgia Archives
Essential Records Course

Participant Guide

2024

Handout 1.1—Essential Records

PRIORITY FOR ACCESS*	ESSENTIAL RECORDS ARE RECORDS THAT:	EXAMPLES INCLUDE:
Priority 1: First 1–12 hours	Are necessary for emergency response	• Copy of emergency and/or Continuity of Operations (COOP) Plan • Infrastructure and utility plans • Maps and building plans • Emergency contact information
	Are necessary to resume or continue operations	• Delegations of authority • Contracts and leases • Payroll • Prison, jail, and parole records • Insurance records
Priority 2: First 12–72 hours	Protect the health, safety, property, and rights of residents	• Deeds, mortgages, land records • Birth and marriage records • Medical records • Active court proceedings • Education and military service records • Voting records • Professional licenses
	Would require massive resources to reconstruct	• Geographic information systems data • Tax records
Priority 3: After first 72 hours	Document the history of communities and families	• Historical documents • Photographs • Identity records

- Only a small percentage (typically, less than five percent) of all Government records are essential
- Value during an emergency makes a record essential
- As disruption time increases, more records become essential
- "Records" can be in many different formats, including paper or electronic

* See **Handout 4.1**—Access Priorities Table for details on what is covered in each of these priority categories.

Caring for Records

Care for your family records

Guidelines for the Careful Handling of Photographic Images

Guidelines for the Careful Handling of Documents

Guidelines for the Careful Handling of Books

Guidelines for the Storage Environment for Records

Guidelines for Selecting Storage Supplies

Vendors - List of commercial vendors of archival supplies.

Disaster Preparedness

Essential Records for Families - Safeguarding the records that protect your family's health, identity, and financial resources

Pocket Response Plan (PReP) - The Council of State Archivists (CoSA) developed this template as part of its Emergency Preparedness Initiative. Side A is an Emergency Communications Plan and Side B provides an Emergency Response Checklist. It can be downloaded in Microsoft Word or as a fillable PDF and customized for any organization, then printed double-sided on a sheet of legal-size paper, trimmed and folded to fit into a Tyvek envelope that will fit in a wallet.

Emergency Response

Disaster Resources for the Public, part of Heritage Emergency National Task Force A website with disaster resources for the public in case of hurricane

Mitigating Potential Hazards to Materials and Individuals Following a Disaster - Includes links to health assistance and information and disaster preparedness and prevention.

CONTACT INFORMATION

Address: 5800 Jonesboro Road
Morrow, GA 30260

Phone: 678-364-3710

Hours: Tuesday - Saturday
9:00 AM - 12:00 PM
and 1:00PM - 4:00PM
Closed 12:00 - 1:00

Social:

FEATURED CONTENT

The Georgia Archives website located at *GeorgiaArchives.org* includes copies of the course materials under the CARING FOR RECORDS tab of the Georgia Archives website along with the other useful emergency preparedness and disaster response resources you can find there. The course materials will be available for the next couple of weeks on the Georgia Archives site.

Slide 1-8

This course supports a fundamental component of Continuity of Operations (COOP):

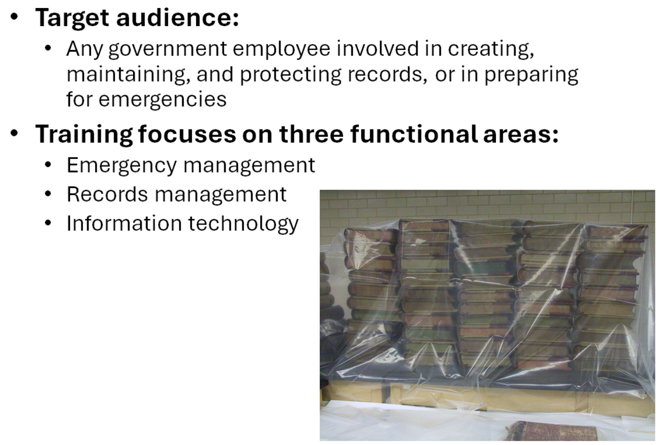
- Ensuring that state and local governments can access and use records needed to restore essential services

2014 Hancock County, GA, Courthouse Fire Aftermath – Photo courtesy of GA Archives

Notice: This course supports a fundamental component of Continuity of Operations (COOP): ensuring that state and local governments can access and use records—both paper and electronic—needed to restore essential services and functions after a disaster or emergency. The statements made in this document, on the slides, and by presenters are for this purpose. Always follow the policies, procedures, and laws governing your organization and its actions.

This course will also help state and local agencies identify other records that need protection because they have long-term legal, administrative, or cultural value. These records include those that define people’s rights, document government obligations, secure your community’s economic well-being, and provide community identity.

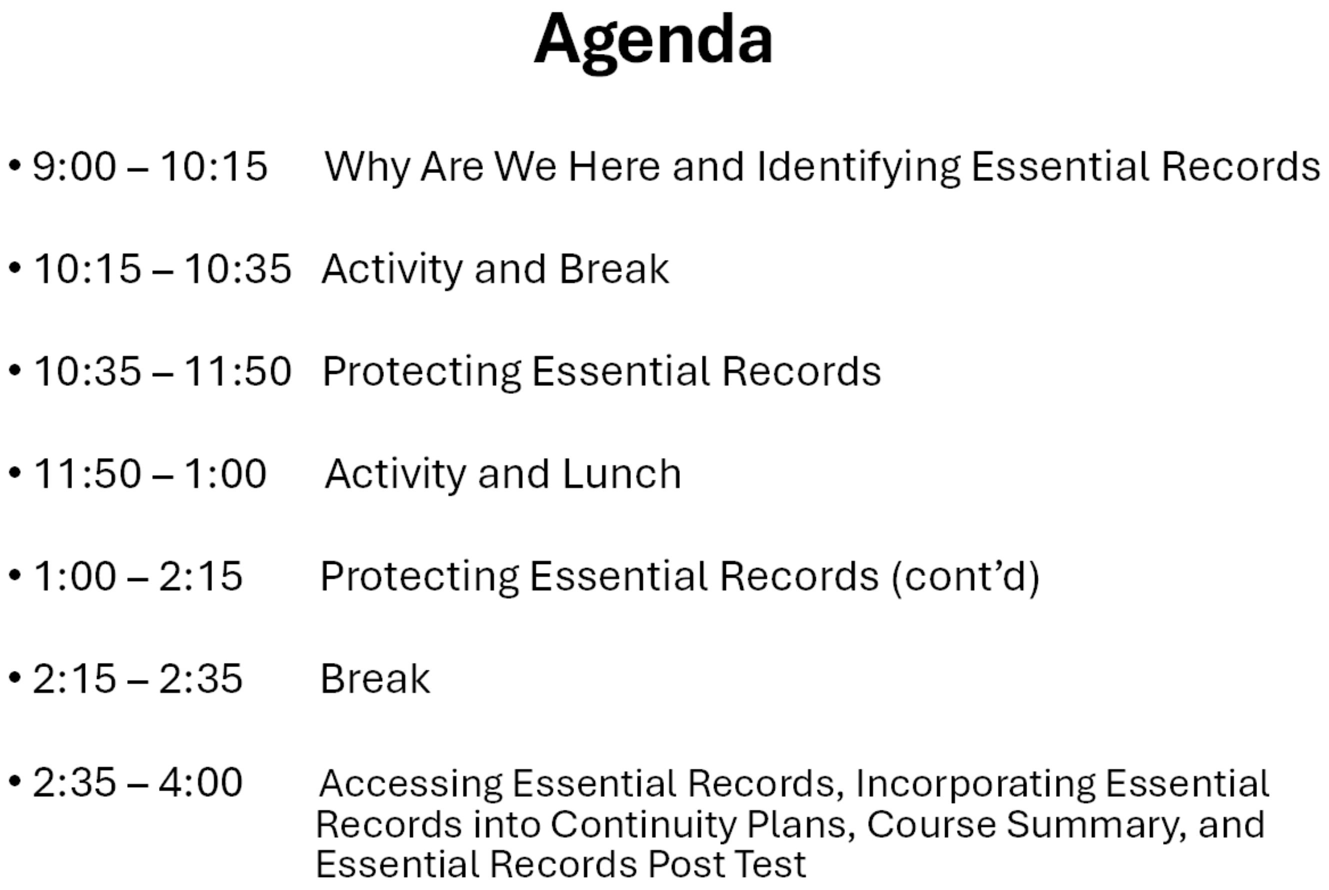
Slide 1-9



- **Target audience:**
  - Any government employee involved in creating, maintaining, and protecting records, or in preparing for emergencies
- **Training focuses on three functional areas:**
  - Emergency management
  - Records management
  - Information technology

Course Organization and Agenda

Slide 1-10



Agenda

- 9:00 – 10:15 Why Are We Here and Identifying Essential Records
- 10:15 – 10:35 Activity and Break
- 10:35 – 11:50 Protecting Essential Records
- 11:50 – 1:00 Activity and Lunch
- 1:00 – 2:15 Protecting Essential Records (cont'd)
- 2:15 – 2:35 Break
- 2:35 – 4:00 Accessing Essential Records, Incorporating Essential Records into Continuity Plans, Course Summary, and Essential Records Post Test

The Curriculum

The curriculum consists of two primary courses that have complementary content and are designed to be taken sequentially.

In the *Essential Records* course, participants will learn to:

- Define an essential record
- Identify an organization's critical business needs and functions and the records that are essential to support those functions
- Evaluate the hazards and risks that most threaten your agency's essential records
- Develop appropriate protection strategies against these threats
- Specify time frames in which access will be needed to specific records
- Develop procedures to ensure that essential records remain both accessible and secure
- Develop an essential records template that can be incorporated into a broader Continuity Plan and/or emergency plan
- Understand applicable federal, state, and local Continuity regulations and procedures

In the *Emergency Planning and Response* for Essential Records course, participants will learn to:

- Understand the benefits of records emergency planning
- Relate records emergency planning to Continuity Plans and procedures
- Develop, analyze, and test a Records Emergency Action Plan (REAP)
- Assess the damage to records after an emergency and implement a response
- Identify federal, state, and local resources that are available to assist when an emergency occurs

Also part of the Georgia Archives curriculum is a third course—a supporting course—*Introduction to Records Management for State and Local Governments*. This course provides a basic understanding of records management and prepares those with little or no records management experience for the two primary courses.

Why Are We Here?

Slide 1-13

Why Are We Here?

When emergencies strike, records are critically important:

- Emergency responders need records to respond to the situation and to continue operations.
- Government agencies need records to provide essential services.
- Individuals need government records to prove their identity and re-establish their lives.

Slide 1-14

Why are we here? (continued)

Slide 1-15

Why are we here? (continued)

Slide 1-16

Why are we here? (continued)

Photo courtesy of University of Georgia Libraries

Slide 1-17

Why are we here? (continued)

During and after an emergency, the ability to access critical records and information quickly and easily is a major function of COOP. However, too often the COOP process emphasizes the physical infrastructure and systems, neglecting the identification and protection of essential records.

Records custodians must be prepared to protect their essential records so that, in the event of an emergency, their offices can recover quickly and return to service for the residents of their state or locality.

This course addresses this need by presenting a step-by-step approach to developing an essential records program that is based on FEMA's COOP guidance. In four sessions we will cover identification, protection, accessibility, and implementation of a scalable essential records program. Using assignments designed for you to apply immediately what you've learned to your particular workplace setting, you will develop all the components necessary for a comprehensive essential records program.

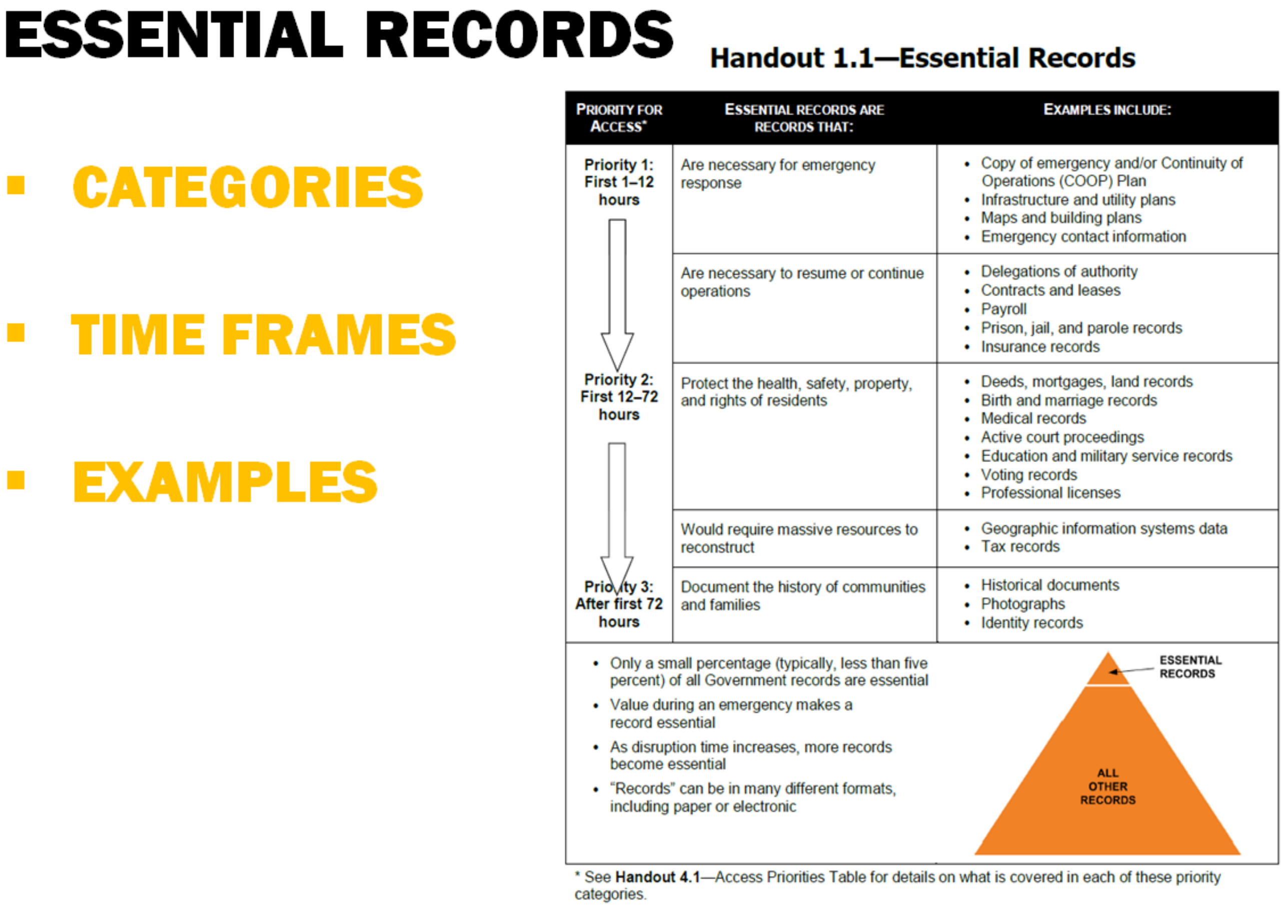
Too often, the COOP process neglects the identification and protection of essential records. Records custodians must be prepared to protect their essential records so that, in the event of an emergency, their offices can recover quickly and return to service for the residents of their state or locality. This Essential Records course presents a step-by-step approach to developing an essential records program.

Session 1—
Identify Essential Records

Session 1 Introduction

Session 1 Overview

Slide 1-19



ESSENTIAL RECORDS

- CATEGORIES
- TIME FRAMES
- EXAMPLES

Handout 1.1—Essential Records

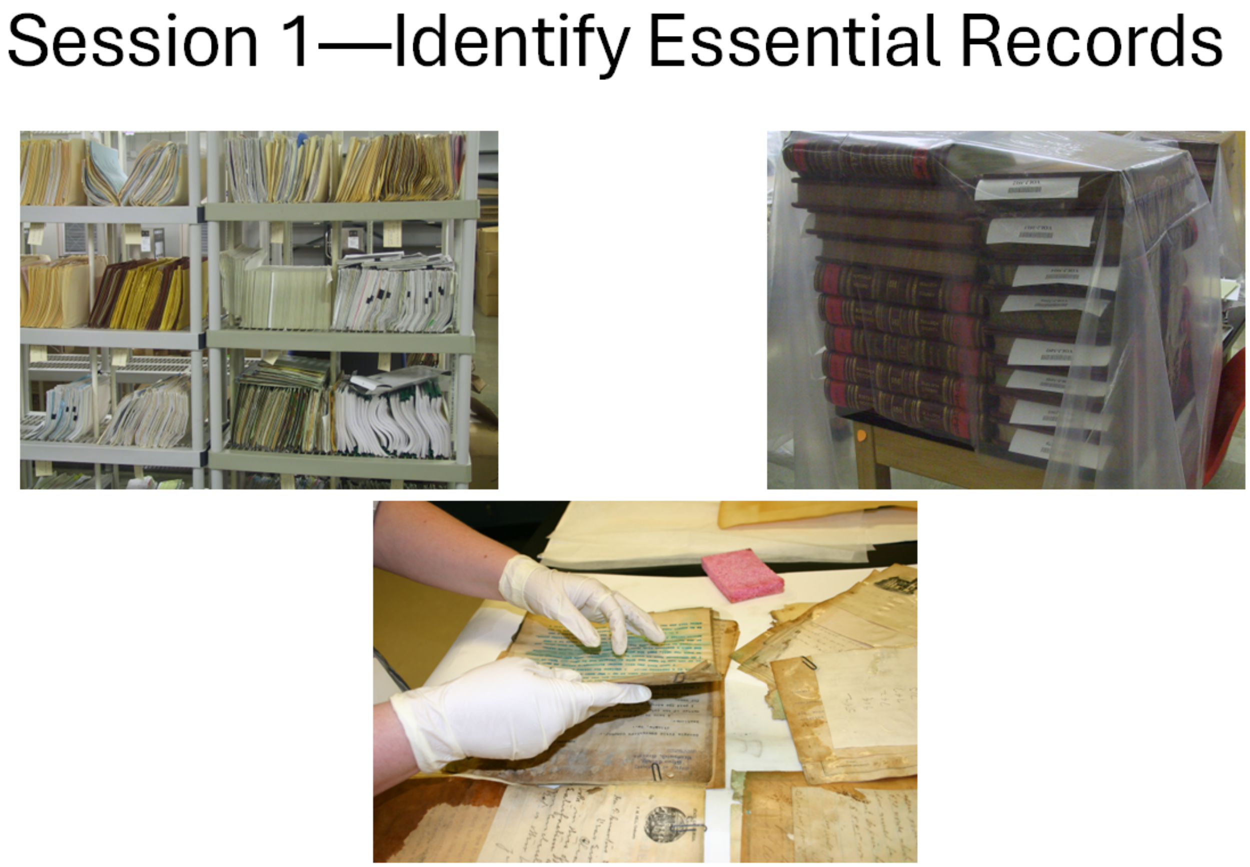
PRIORITY FOR ACCESS*	ESSENTIAL RECORDS ARE RECORDS THAT:	EXAMPLES INCLUDE:
Priority 1: First 1–12 hours	Are necessary for emergency response	• Copy of emergency and/or Continuity of Operations (COOP) Plan • Infrastructure and utility plans • Maps and building plans • Emergency contact information
	Are necessary to resume or continue operations	• Delegations of authority • Contracts and leases • Payroll • Prison, jail, and parole records • Insurance records
Priority 2: First 12–72 hours	Protect the health, safety, property, and rights of residents	• Deeds, mortgages, land records • Birth and marriage records • Medical records • Active court proceedings • Education and military service records • Voting records • Professional licenses
	Would require massive resources to reconstruct	• Geographic information systems data • Tax records
Priority 3: After first 72 hours	Document the history of communities and families	• Historical documents • Photographs • Identity records

- Only a small percentage (typically, less than five percent) of all Government records are essential
- Value during an emergency makes a record essential
- As disruption time increases, more records become essential
- "Records" can be in many different formats, including paper or electronic

* See **Handout 4.1**—Access Priorities Table for details on what is covered in each of these priority categories.

Session 1 Introduction

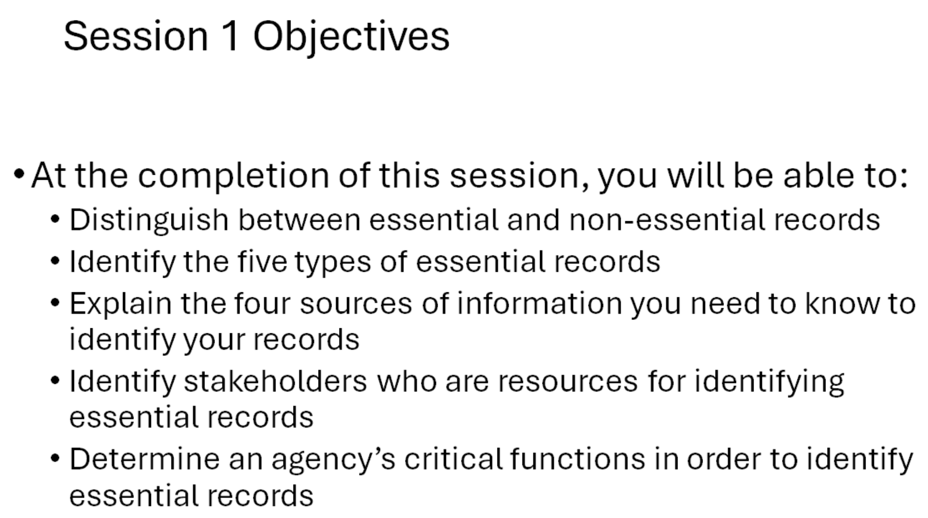
Slide 1-20



Session 1—Identify Essential Records

Session 1 Objectives

Slide 1-21



Session 1 Objectives

- At the completion of this session, you will be able to:
  - Distinguish between essential and non-essential records
  - Identify the five types of essential records
  - Explain the four sources of information you need to know to identify your records
  - Identify stakeholders who are resources for identifying essential records
  - Determine an agency’s critical functions in order to identify essential records

Lesson 1: What are Essential Records

Slide 1-22

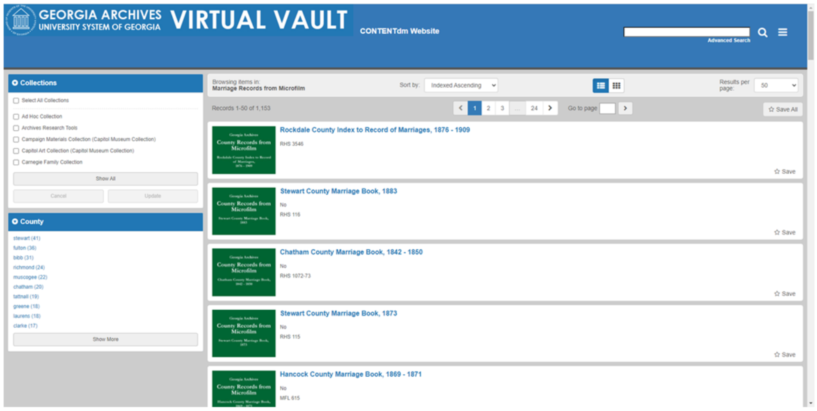
What Are Essential Records?

- Records are considered essential when they:
  - Are necessary for emergency response
  - Are necessary to resume or continue operations
  - Protect the health, safety, property, and rights of residents
  - Would require massive resources to reconstruct
  - Document the history of communities and families (and agencies)

Slide 1-23

What Are Essential Records? (continued)

- Essential records require special protection strategies to ensure they are protected and accessible.
- Essential records can be found in any format and in any medium.



☐ Select All Collections
☐ Ad Hoc Collection
☐ Archives Research Tools
☐ Campaign Materials Collection (Capitol Museum Collection)
☐ Capitol Art Collection (Capitol Museum Collection)
☐ Carnegie Family Collection

stewart (41)
fulton (36)
bibb (31)
richmond (24)
muscogee (22)
chatham (20)
tattnall (19)
greene (18)
laurens (18)
clarke (17)

Browsing items in:
Marriage Records from Microfilm

Sort by: Indexed Ascending

Results per page: 50

Records 1-50 of 1,153

1 2 3 ... 24

Go to page

Rockdale County Index to Record of Marriages, 1876 - 1909
RHS 3546

Stewart County Marriage Book, 1883
No
RHS 116

Chatham County Marriage Book, 1842 - 1850
No
RHS 1072-73

Stewart County Marriage Book, 1873
No
RHS 115

Hancock County Marriage Book, 1869 - 1871
No
MFL 615

Essential records provide the agency with information it needs to conduct business under other-than-normal conditions, and to resume more normal business afterwards. These records, combined with other components of a business continuity plan, allow the agency to continue functioning under a range of adverse conditions, whatever their intensity and duration.

We use the term “essential records” in this course, but these records also go by other names. The federal government refers to them as “vital records” and the business community often calls them “mission-critical or business-critical records.” We use “essential records” as synonymous with all of these terms.

Records are considered essential when they:

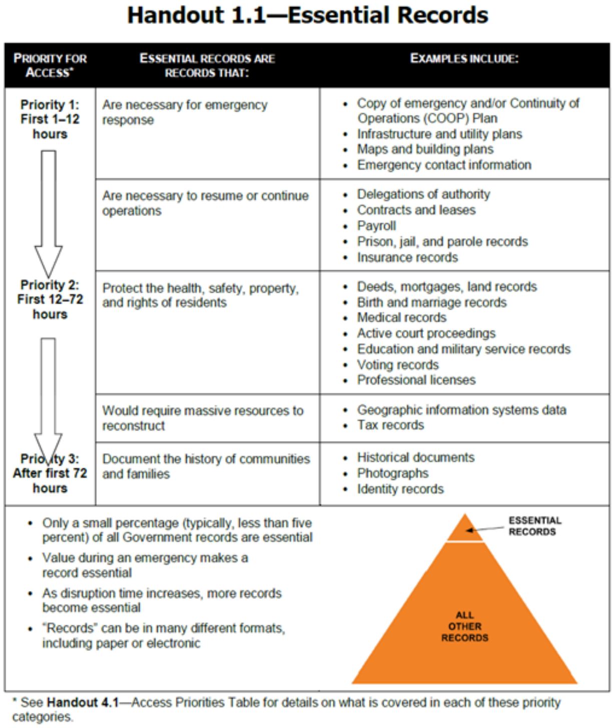
- Are necessary for emergency response
- Are necessary to resume or continue operations
- Protect the health, safety, property, and rights of residents
- Would require massive resources to reconstruct
- Document the history of communities and families

Handout 1.1—Essential Records provides examples of records that fall into each of these five categories.

Agencies must be prepared to cope with a wide range of emergencies, from fires or plumbing failures that might affect a single building, to natural emergencies, pandemics, and power failures that could affect a broad geographic area. In every case, certain records are critical to the agency and to those who depend on it for services.

Essential records require special protection strategies, such as backing up systems, or copying and dispersing files and resources off site. These strategies ensure that essential records are not only protected from the effects of an emergency, but are also accessible during and after an emergency.

Essential records can be found in any format and in any medium—paper, electronic, microfilm, photographs, and more. Essential records are considered to be essential based on the information they contain, not on their format.



Handout 1.1—Essential Records

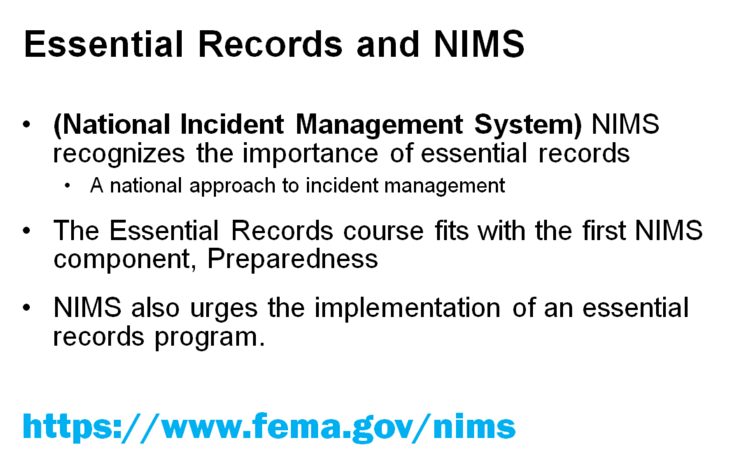
Priority for Access*	Essential Records are Records That:	Examples Include:
Priority 1: First 1–12 hours	Are necessary for emergency response	• Copy of emergency and/or Continuity of Operations (COOP) Plan • Infrastructure and utility plans • Maps and building plans • Emergency contact information
	Are necessary to resume or continue operations	• Delegations of authority • Contracts and leases • Payroll • Prison, jail, and parole records • Insurance records
Priority 2: First 12–72 hours	Protect the health, safety, property, and rights of residents	• Deeds, mortgages, land records • Birth and marriage records • Medical records • Active court proceedings • Education and military service records • Voting records • Professional licenses
	Would require massive resources to reconstruct	• Geographic information systems data • Tax records
Priority 3: After first 72 hours	Document the history of communities and families	• Historical documents • Photographs • Identity records

- Only a small percentage (typically, less than five percent) of all Government records are essential
- Value during an emergency makes a record essential
- As disruption time increases, more records become essential
- “Records” can be in many different formats, including paper or electronic

* See **Handout 4.1**—Access Priorities Table for details on what is covered in each of these priority categories.

Essential Records and NIMS

Slide 1-24



Essential Records and NIMS

- **(National Incident Management System)** NIMS recognizes the importance of essential records
  - A national approach to incident management
- The Essential Records course fits with the first NIMS component, Preparedness
- NIMS also urges the implementation of an essential records program.

https://www.fema.gov/nims

The importance of essential records is recognized by the federal government in the National Incident Management System (NIMS).

NIMS is a comprehensive, national approach to incident management that is applicable at all jurisdictional levels and across functional disciplines. NIMS enables government entities to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment.

NIMS is **flexible** because it is applicable to any incident regardless of cause, size, location, or complexity, and its components can also be used to develop all-hazards plans, processes, procedures, agreements, and roles.

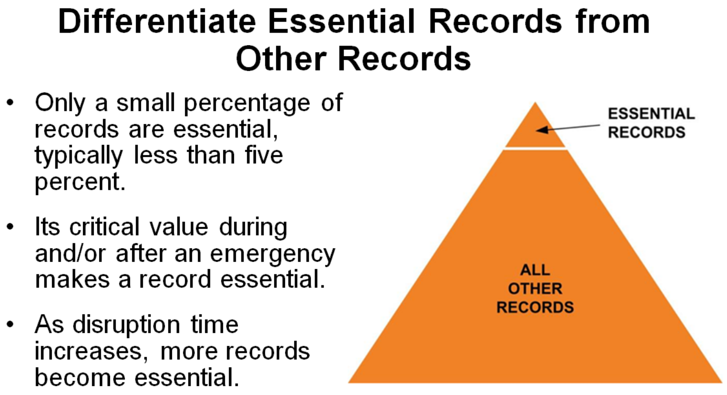
Additionally, NIMS provides an organized set of **scalable** and **standardized** operational structures, which is critical for allowing various organizations and agencies to work together in a predictable, coordinated manner.

NIMS has five different components, and this course fits well with the first component, Preparedness. NIMS specifically urges elected and appointed officials to lead preparedness efforts in their community and agencies.

Preparedness is achieved and maintained through a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action. NIMS also specifically urges the implementation of an essential records program at all levels of government to prevent loss of crucial documents and records. Refer to **Handout 1.2—NIMS Resource Management Concepts and Principles** for an introduction to NIMS concepts and principles.

Differentiate Essential Records from Other Records

Slide 1-25



Differentiate Essential Records from Other Records

- Only a small percentage of records are essential, typically less than five percent.
- Its critical value during and/or after an emergency makes a record essential.
- As disruption time increases, more records become essential.

Determining which of your records are "essential" requires a great deal of thought, and opinions will vary widely. All records are useful to the agency in some way; however, only a small percentage—typically less than five percent, government-wide—are essential. However, some agencies, such as court clerks and county recorders, may legitimately designate a more substantial percentage as essential.

Throughout this course, we will be examining in detail the factors that will help you make the decision as to whether a record is an essential record, including:

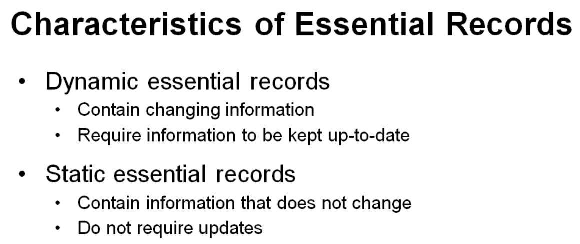
- Mission-critical functions of your agency
- Costs (time, money, operational, and human) associated with potential loss
- The speed with which you will need to access the records when an emergency occurs
- Ability to reconstruct record

Its critical value during and/or after an emergency is what makes a record essential, and these four factors determine the critical value of a record.

As disruption time increases, more records become essential.

Characteristics of Essential Records

Slide 1-26



Characteristics of Essential Records

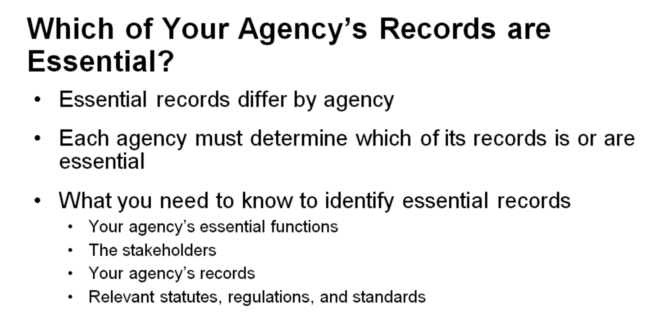
- Dynamic essential records
  - Contain changing information
  - Require information to be kept up-to-date
- Static essential records
  - Contain information that does not change
  - Do not require updates

Essential records are either dynamic or static:

- Dynamic essential records contain information that can change periodically—for example, phone trees, in which the phone numbers and contact names may change over time. In order to be useful in an emergency, dynamic essential records must be kept up-to-date. This requires actively validating the information in the record and making updates as changes occur.
- Static essential records contain information that does not change over time—for example, birth records and the results of elections. Because the record's information doesn't change, these records do not require updates.

Which of Your Agency's Records Are Essential?

Slide 1-27



Which of Your Agency's Records are Essential?

- Essential records differ by agency
- Each agency must determine which of its records is or are essential
- What you need to know to identify essential records
  - Your agency's essential functions
  - The stakeholders
  - Your agency's records
  - Relevant statutes, regulations, and standards

Essential records differ from agency to agency—there is no master list of all the records that an agency should deem essential. Each agency must determine for itself the records required to respond to an emergency and continue operations. While federal and state laws and regulations may establish general categories of records deemed to be essential, matching those categories to specific records series in each agency must be done by those who know both the records and the agency's functions very well.

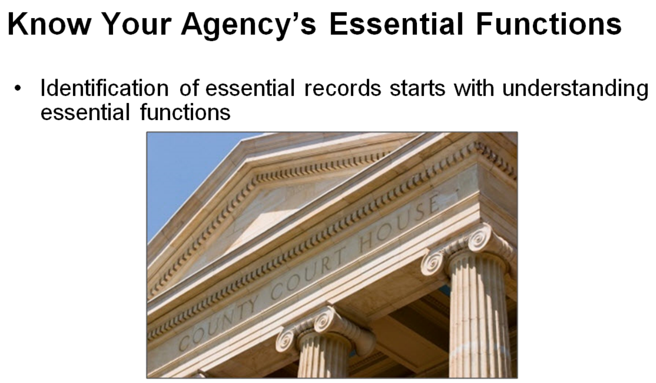
Bottom line: No one can define for you which of your records is or are essential.

To identify your essential records, there are four pieces of information you need to know:

- Your agency's essential functions
- Your stakeholders
- Your agency's records
- Relevant statutes, regulations, and standards

Know Your Agency’s Essential Functions

Slide 1-28



Know Your Agency’s Essential Functions

- Identification of essential records starts with understanding essential functions

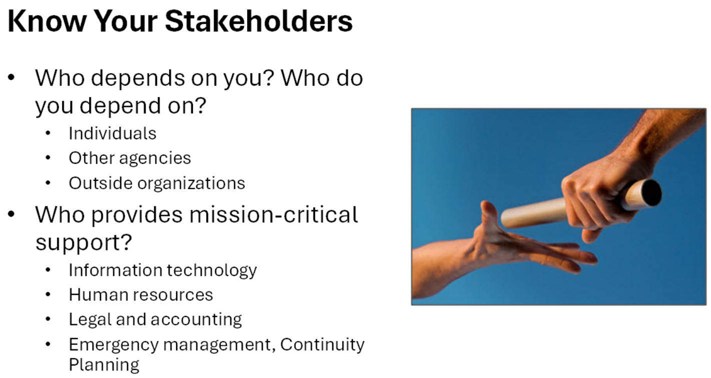
COUNTY COURT HOUSE

The identification of essential records starts with understanding the essential functions of your agency, its departments, and its programs. This must be done in close consultation with people up and down and across the agency, as well as with stakeholders from the outside.

Once you’ve identified the essential functions, you can determine which of those functions your agency must continue to perform regardless of operating conditions. From there you will be able to determine the records needed to support those functions—i.e., your essential records.

Know the Stakeholders

Slide 1-29



Know Your Stakeholders

- Who depends on you? Who do you depend on?
  - Individuals
  - Other agencies
  - Outside organizations
- Who provides mission-critical support?
  - Information technology
  - Human resources
  - Legal and accounting
  - Emergency management, Continuity Planning

Another way to identify your essential records is to know the people who have an interest in identifying and protecting your agency's essential records.

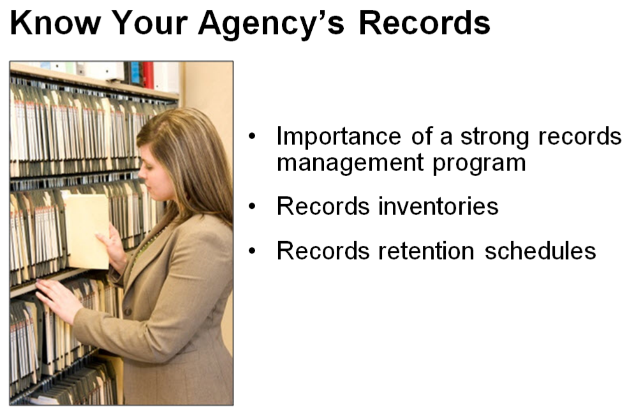
Talk to the people who depend on your agency's services. These stakeholders can help you understand which of your services are essential to them and why. This, in turn, will help you identify the records that support those services. You'll want to consult with other agencies or outside organizations that come to you often for information or services, because they can help you identify which records are essential to their operations and cannot be found elsewhere. Likewise, one of the most important considerations is the public and its requirements. Residents of your state or locality depend on the government to retain critical information needed to sustain their families and businesses, and to make that information available when needed.

Also talk to the people you depend on in order to provide services. If your agency depends on records in other organizations to support your ongoing operations, you'll want to ensure that that agency's records will remain available during an emergency, or you'll want to make provisions to obtain critical information elsewhere. If, for instance, you depend on certain computer systems, but those systems are managed and maintained by people outside your office, you need to talk to the custodians of those systems to identify records that are essential to you but may not be under your control (such as system documentation, for example).

Additional stakeholders you'll want to consult with include mission-critical program or department heads, the Information Technology (IT) Director, Human Resources (HR), Legal staff and senior executives, and others. Later, the Continuity Manager and Emergency Manager for your agency should be consulted, so that they see how to integrate your work with the current plan and emergency training. The agency head (or designee) and IT Director should be briefed fully on aspects of your plan that will require resources—especially those recommendations for protecting records.

Know Your Agency's Records

Slide 1-30



Know Your Agency's Records

- Importance of a strong records management program
- Records inventories
- Records retention schedules

Selection of essential records is based on comprehensive knowledge of all the agency's records. Most state and local governments mandate specific records management practices through laws, regulations, or administrative rules. These practices and the documents that result provide the comprehensive knowledge of an agency's records.

A well-developed records management program can go a long way toward protecting and accessing essential records in an emergency. In addition to ensuring that best practices are followed for the storage and reproduction of records, two documents at the heart of a proper records management program will help you identify essential records:

- **Records inventories** are basic tools of records management—you can't manage something unless you know what you have and where it is. The inventory is also the foundation for every effective Essential Records Program. A records inventory is a complete and accurate survey of an agency's business information that documents the function, flow, and description of records. Paper records are inventoried by record series. Electronic records are inventoried by information systems. To be effective, an inventory should take into account records in all media, including records in all media, including paper, microfilm, microfiche, photographs, and electronic formats, if they are part of the same process, to ensure that the relationships between them can be fully identified.

- **Records retention schedules** systematically identify and describe all the records in an agency (often from information gathered during a records inventory), specify how long they should be retained, and designate certain records as permanent. Permanent records, generally speaking, are essential because they meet one of the five criteria we spoke of earlier (see “What Are Essential Records?” topic). Generally, they are not needed in the first hours or days of an emergency, but their long-term value requires that they be protected. We will talk about this later in the course.

Records retention schedules can help you understand who creates specific records and how they are used.

Increasingly, essential records are being flagged in retention schedules, so starting with the retention schedule as a source for identifying essential records may save you a great deal of time.

The Georgia Archives is responsible for working with state and local agencies to produce and submit retention schedules to the State Records Committee.

Copies of approved schedules are located at www.georgiaarchives.org/records/retention_schedules

The official definition of Records Management:

- O.C.G.A. § 50-18-91: "Records management" means the application of management techniques to the creation, utilization, maintenance, retention, preservation, and disposal of records undertaken to reduce costs and improve efficiency of record keeping. "Records management" includes management of filing and microfilming equipment and supplies; filing and information retrieval systems; files, correspondence, reports, and forms management; historical documentation; micrographics; retention programming; and vital records protection.

The official definition of Public Records:

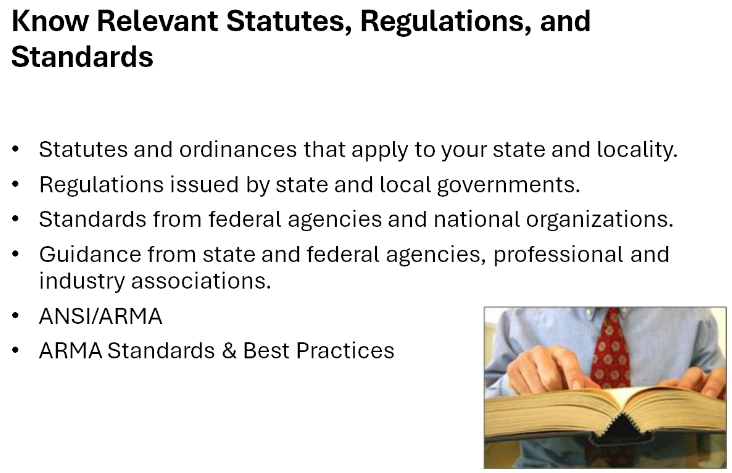
- O.C.G.A. § 50-18-91: “Records" means all documents, papers, letters, maps, books (except books in formally organized libraries), microfilm, magnetic tape, or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in performance of functions by any agency.

Information regarding a "Records Management Officer" is under Opinions of the Attorney General regarding O.C.G.A. § 50-18-92.

- Stated "Agency head has direct supervisory control over the agency records management officer and, subject to the approval of the State Records Committee, direct control over the agency’s records management program. 1975 Op. Att'y Gen. No. 75-84."

Know the Relevant Statutes, Regulations, and Standards

Slide 1-31



Know Relevant Statutes, Regulations, and Standards

- Statutes and ordinances that apply to your state and locality.
- Regulations issued by state and local governments.
- Standards from federal agencies and national organizations.
- Guidance from state and federal agencies, professional and industry associations.
- ANSI/ARMA
- ARMA Standards & Best Practices

Statutes and Regulations

Statutes and regulations addressing emergency management and records management typically include directives on identifying and protecting essential records. When identifying essential records, it’s important to know the statues and regulations that apply to your agency, so that you can ensure that you meet your agency’s operational and legal requirements. While statutes and regulations don’t often address essential records directly, the laws assume that you will protect the resources—including records—you need to meet your legal obligations.

Standards

You should also be aware of the industry standards for essential records, as they provide useful information to help identify essential records.

Some examples of industry standards for essential records are:

- ANSI/ARMA 5-2003 “Vital Records Programs: Identifying, Managing, and Recovering Business Critical Records” https://webstore.ansi.org/standards/arma/ansiarma2003?srsltid=AfmBOorJ_9ynwaj2PaQpsu0KtNhcHi2dfVTDzst5A_kNlgmrg23JMlaT

- ARMA's “Standards and Best Practices” *http://www.arma.org/standards/VitalRecords.cfm*

The Georgia Archives can discuss standards and/or best practices that will help you identify and protect essential records.

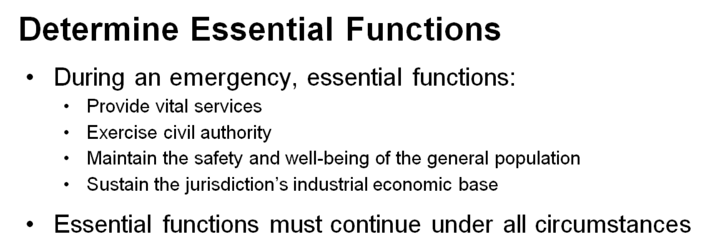
Refer to state laws and regulations addressing emergency management and records management.

Refer to **Handout 1.3—Potential Candidates for Essential Records Status** to help you start thinking about the records in your agency that may be essential records.

Lesson 2: Identify Essential Records by Examining Functions

Determine Essential Functions

Slide 1-32



Determine Essential Functions

- During an emergency, essential functions:
  - Provide vital services
  - Exercise civil authority
  - Maintain the safety and well-being of the general population
  - Sustain the jurisdiction's industrial economic base
- Essential functions must continue under all circumstances

Essential functions are the functions that enable a government to provide vital services, exercise civil authority, maintain the safety and well-being of the general population, and sustain its jurisdiction's industrial and economic base in an emergency.

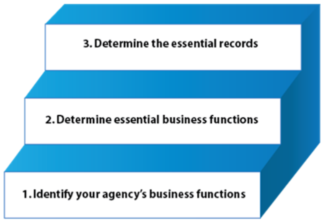
These functions must continue under all circumstances with minimal disruption, and cannot be interrupted for even a short period of time without compromising the agency's ability to perform its mission.

It is the responsibility of your agency's Continuity team to determine the essential functions of your agency. Be sure to review the Continuity Plan before you start identifying essential functions, because the Continuity Manager may already have accomplished this task.

Slide 1-33

Determine Essential Functions (continued)

Steps to determine essential functions


3. Determine the essential records
2. Determine essential business functions
1. Identify your agency's business functions

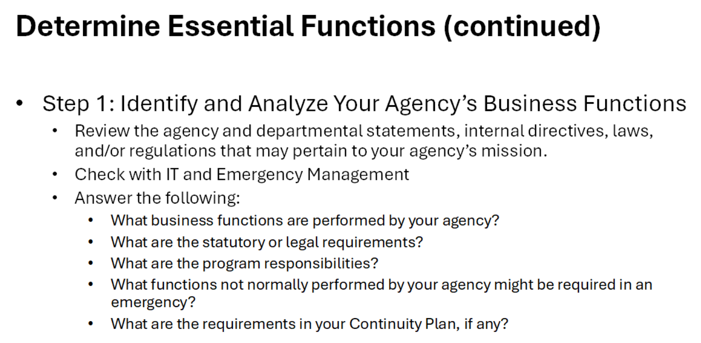
If a Continuity Plan or team has not been established for your agency, and you have been tasked with coordinating an Essential Records Program, follow these steps to determine your agency's essential functions:

1. Identify and analyze your agency's business functions.
2. Determine essential business functions.
3. Determine the essential records that support those functions.

Let's look at each of these steps in detail.

Step 1: Identify and Analyze Your Agency’s Business Functions

Slide 1-34



Determine Essential Functions (continued)

- Step 1: Identify and Analyze Your Agency’s Business Functions
  - Review the agency and departmental statements, internal directives, laws, and/or regulations that may pertain to your agency’s mission.
  - Check with IT and Emergency Management
  - Answer the following:
    - What business functions are performed by your agency?
    - What are the statutory or legal requirements?
    - What are the program responsibilities?
    - What functions not normally performed by your agency might be required in an emergency?
    - What are the requirements in your Continuity Plan, if any?

In this phase, you are gathering comprehensive information about your agency’s business functions by reviewing agency and departmental statements, internal directive, laws, and/or regulations that pertain to your agency’s mission.

At this point, you should also check with IT and Emergency Management to see if they have already undertaken any contingency planning or BIA (Business Impact Assessment) activity. These analyses result in identification of essential agency functions and can save you much time if they already exist. You can find more information about the BIA process on the IPER Resource Center.

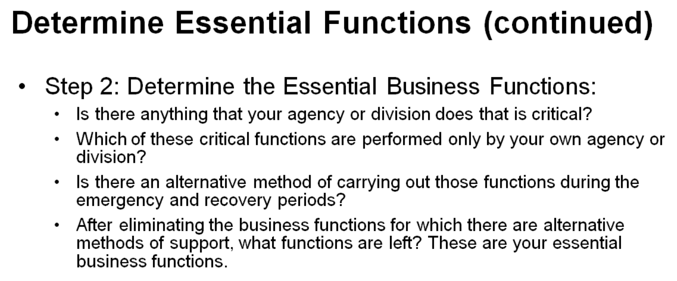
Your information-gathering will seek to answer the following questions about your agency:

- What business functions are performed by your agency?
  - What is the purpose of the agency? Of each department?
  - What is the agency’s major function? Each department’s major function?
- What are the statutory or legal requirements?
- What are the program responsibilities?
- What functions not normally performed by your agency might be required in an emergency?
- What are the requirements in your Continuity Plan, if any?

Keep in mind that business functions do not necessarily mean only those functions transacted between the agency and the public. Business functions also refer to those functions performed between agencies.

Step 2: Determine the Essential Business Functions

Slide 1-35



Determine Essential Functions (continued)

- Step 2: Determine the Essential Business Functions:
  - Is there anything that your agency or division does that is critical?
  - Which of these critical functions are performed only by your own agency or division?
  - Is there an alternative method of carrying out those functions during the emergency and recovery periods?
  - After eliminating the business functions for which there are alternative methods of support, what functions are left? These are your essential business functions.

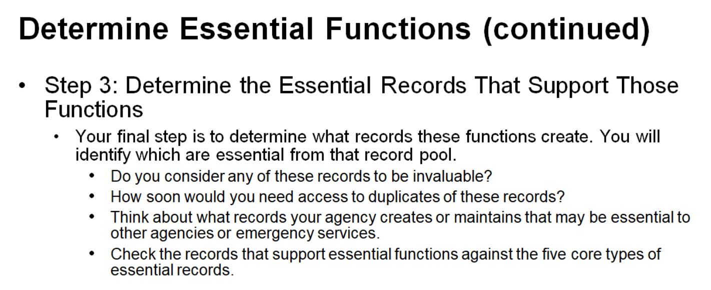
Once you have identified the business functions, you will need to analyze and prioritize them based on what functions your agency, and the government as a whole, must perform under adverse operating conditions.

1. Is there anything that your own agency or division does that is critical to the larger agency or government of which it is a part? That is, if your operation were shut down because of an emergency, how greatly would that affect the rest of your organization, other agencies, the government as a whole, or the public?
2. Which of these critical functions is or are performed only by your own agency or division and not also done elsewhere?
   - Keep in mind the importance of each function:
     - Does it ensure uninterrupted communication, responsibility, and leadership of the department?
     - Does it protect critical facilities, systems, equipment, and records?
     - Does it continue to pay the government's obligations?
3. For the functions that are essential to your agency and are not done elsewhere, is there an alternative method of carrying out those functions during the emergency and recovery periods (regardless of how inefficient the alternative method may be)?
4. After eliminating the business functions for which there are alternative methods of support, what functions are left? These functions constitute your essential business functions.

NOTE: You should continue to monitor any essential functions that you have eliminated because they have alternative support. Changing circumstances may mean that your agency will have to resume responsibility for those functions in the future and will once again need records to support them.

Step 3: Determine the Essential Records That Support Those Functions

Slide 1-36



Determine Essential Functions (continued)

- Step 3: Determine the Essential Records That Support Those Functions
  - Your final step is to determine what records these functions create. You will identify which are essential from that record pool.
    - Do you consider any of these records to be invaluable?
    - How soon would you need access to duplicates of these records?
    - Think about what records your agency creates or maintains that may be essential to other agencies or emergency services.
    - Check the records that support essential functions against the five core types of essential records.

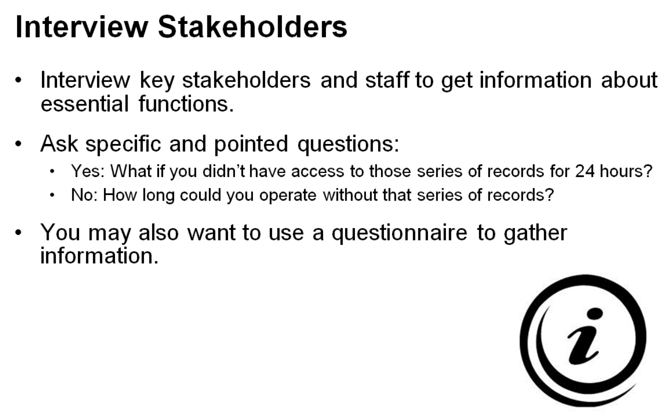
Your final step is to determine what records are created by those essential functions, because this will be the pool of records from which your essential records will come.

- Do you consider any of these records to be invaluable? That is, if one or more of these records were lost because of an emergency, or were unavailable during an emergency, would there be any dramatic effect on your agency's ability to perform its critical functions? Any effect on the rest of your agency's operation? Any effect on other agencies or the public?
- Are there records that you create or maintain that the public would need in an emergency?
- How soon would you need access to duplicates of these records if one or more of the original records were lost or unavailable because of the emergency?
- Also think about what records your agency creates or maintains that may be essential to other agencies or emergency services but are NOT essential to your essential functions—for example, the floor plan of your agency or building plans.
- For a final determination, check the records that support essential functions against the five core types of essential records listed in Lesson 1:
  - Are they necessary for emergency response?
  - Are they necessary to resume or continue operations?
  - Do they protect the health, safety, property, and rights of residents?
  - Would it require massive resources to reconstruct them?
  - Do they document the history of families and communities?

Refer to **Handout 1.4—Examples of Information/Records, by Function, That Might Be Designated as Essential**, for a list of records commonly found in an agency that may be deemed critical to continuity of operations.

Interview Stakeholders

Slide 1-37



Interview Stakeholders

- Interview key stakeholders and staff to get information about essential functions.
- Ask specific and pointed questions:
  - Yes: What if you didn't have access to those series of records for 24 hours?
  - No: How long could you operate without that series of records?
- You may also want to use a questionnaire to gather information.

In most cases, you won't know the answers to all the questions that have to be asked to identify essential functions, so you will need to interview key stakeholders, including staff members, to find your answers.

When conducting your interviews, it's important to ask specific and pointed questions to get at essential record information. Open-ended questions may not get you the answers you need.

For example, instead of asking, "Can you operate without that series of records?" ask, "What if you didn't have access to that series of records for 24 hours? What would the impact be on other agencies? On the public?"

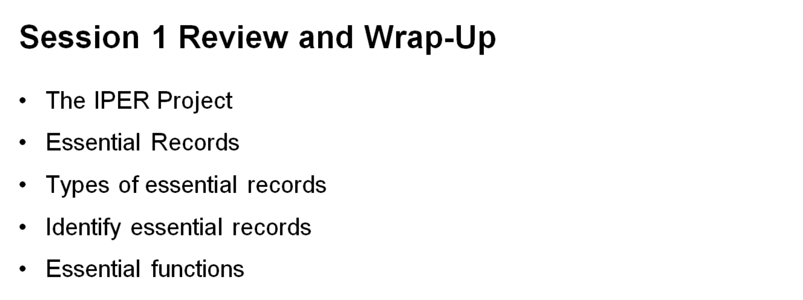
You may want to review with the stakeholders the five categories of essential records described in **Handout 1.1—Essential Records**. This will help determine what needs to be up and running or readily available in the event of an emergency.

You may also want to use a questionnaire to help gather information. Refer to **Handout 1.5—Essential Records Questionnaire** for a sample questionnaire to identify essential functions and records.

Session 1 Review and Wrap-Up

Session Review

Slide 1-38



Session 1 Review and Wrap-Up

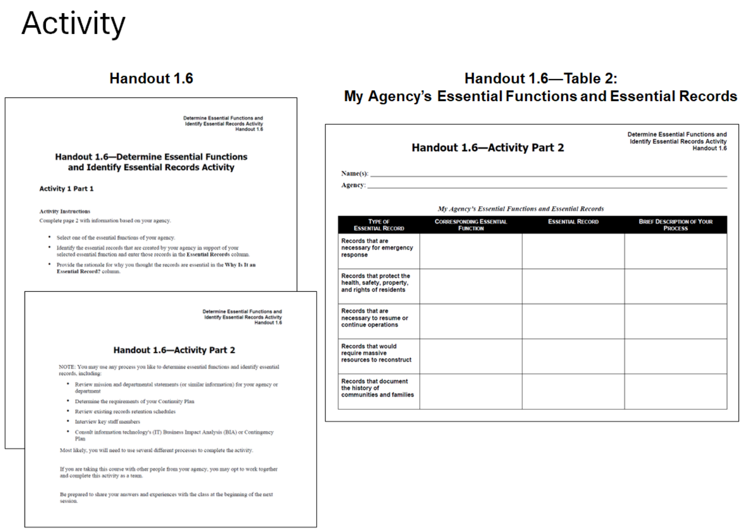
- The IPER Project
- Essential Records
- Types of essential records
- Identify essential records
- Essential functions

In Session 1, you learned:

- About the IPER Project
- The definition of essential records
- The five types of essential records
- That essential records are dynamic or static
- The information needed to identify essential records
- About essential functions and their relationship to essential records
- How to identify essential functions

Activity: Determine Essential Functions and Identify Essential Records

Slide 1-39



Activity

Handout 1.6

Determine Essential Functions and
Identify Essential Records Activity
Handout 1.6

Handout 1.6—Determine Essential Functions and Identify Essential Records Activity

Activity 1 Part 1

Activity Instructions

Complete page 2 with information based on your agency.

- Select one of the essential functions of your agency.
- Identify the essential records that are created by your agency in support of your selected essential function and enter those records in the **Essential Records** column.
- Provide the rationale for why you thought the records are essential in the **Why Is It an Essential Record?** column.

Determine Essential Functions and
Identify Essential Records Activity
Handout 1.6

Handout 1.6—Activity Part 2

NOTE: You may use any process you like to determine essential functions and identify essential records, including:

- Review mission and departmental statements (or similar information) for your agency or department
- Determine the requirements of your Continuity Plan
- Review existing records retention schedules
- Interview key staff members
- Consult information technology's (IT) Business Impact Analysis (BIA) or Contingency Plan

Most likely, you will need to use several different processes to complete the activity.

If you are taking this course with other people from your agency, you may opt to work together and complete this activity as a team.

Be prepared to share your answers and experiences with the class at the beginning of the next session.

Handout 1.6—Table 2:
My Agency's Essential Functions and Essential Records

Determine Essential Functions and
Identify Essential Records Activity
Handout 1.6

Handout 1.6—Activity Part 2

Name(s): ______________________

Agency: ______________________

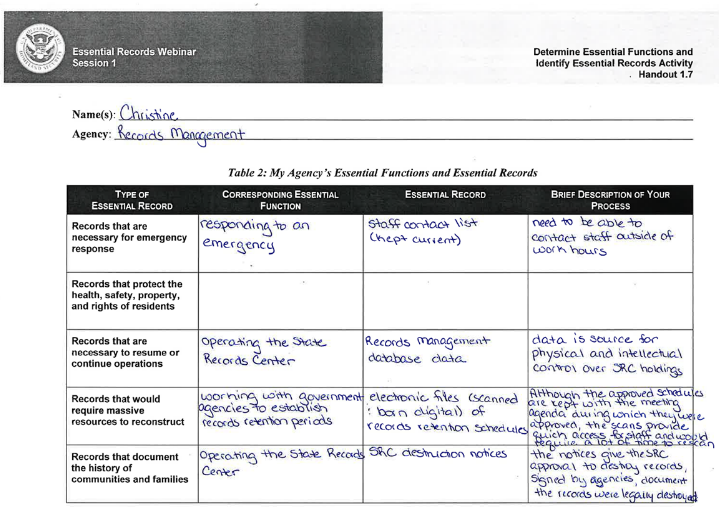
My Agency's Essential Functions and Essential Records

Type of Essential Record	Corresponding Essential Function	Essential Record	Brief Description of Your Process
Records that are necessary for emergency response			
Records that protect the health, safety, property, and rights of residents			
Records that are necessary to resume or continue operations			
Records that would require massive resources to reconstruct			
Records that document the history of communities and families			

Activity materials:

- **Handout 1.6—**Determine Essential Functions and Identify Essential Records Activity

Slide 1-40



Essential Records Webinar
Session 1

Determine Essential Functions and
Identify Essential Records Activity
Handout 1.7

Name(s): Christine

Agency: Records Management

Table 2: My Agency's Essential Functions and Essential Records

Type of Essential Record	Corresponding Essential Function	Essential Record	Brief Description of Your Process
Records that are necessary for emergency response	responding to an emergency	staff contact list (kept current)	need to be able to contact staff outside of work hours
Records that protect the health, safety, property, and rights of residents			
Records that are necessary to resume or continue operations	Operating the State Records Center	Records management database data	data is source for physical and intellectual control over SRC holdings
Records that would require massive resources to reconstruct	working with government agencies to establish records retention periods	electronic files (scanned : born digital) of records retention schedules	Although the approved schedules are kept with the meeting agenda during which they were approved, the scans provide quick access for staff and would require a lot of time to rescan
Records that document the history of communities and families	Operating the State Records Center	SRC destruction notices	the notices give the SRC approval to destroy records, signed by agencies, document the records were legally destroyed

[This page intentionally left blank.]

Georgia Archives Essential Records Course

Session 2

Participant Guide

2024

Table of Contents

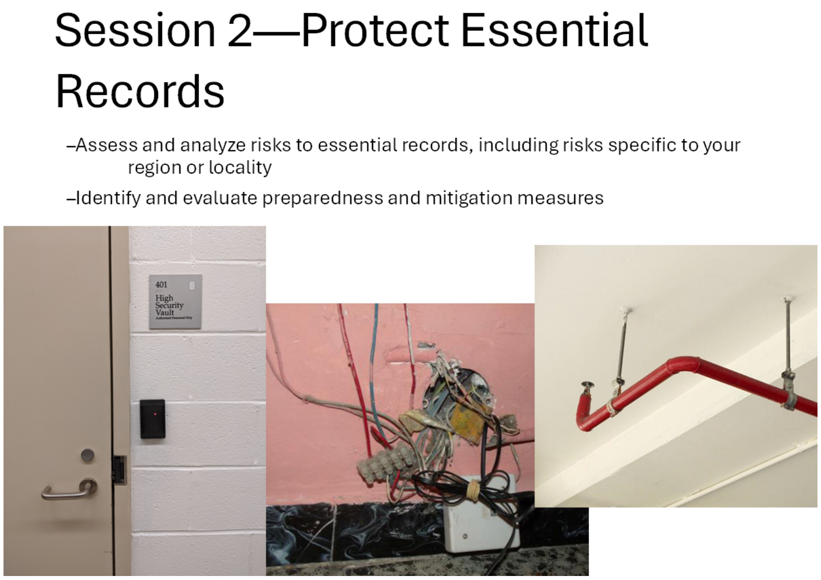
[This page intentionally left blank.]

Session 2—
Protect Essential Records

Session 2 Introduction

Session 2 Introduction and Objectives

Slide 2-7



Session 2—Protect Essential Records

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

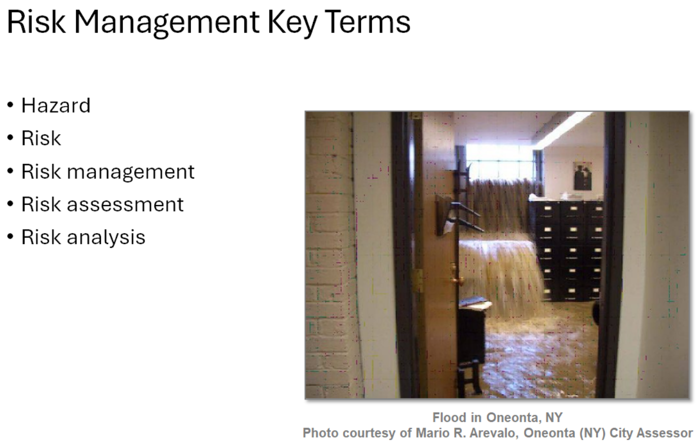
401
High Security Vault

Required materials for Session 2:

- Session 2 Participant Guide
- Session 2 handouts:
  - **Handout 2.1**—Risk Assessment Sample Hazards
  - **Handout 2.2**—Possible Hazards
  - **Handout 2.3**—Identify and Evaluate Risks
- Materials from prior sessions:
  - **Handout 1.6**—Determine Essential Functions and Identify Essential Records Activity

Risk Management Key Terms

Slide 2-8



Risk Management Key Terms

- Hazard
- Risk
- Risk management
- Risk assessment
- Risk analysis

Flood in Oneonta, NY
Photo courtesy of Mario R. Arevalo, Oneonta (NY) City Assessor

You need to be familiar with certain terms in order to discuss protection of your essential records:

- A **hazard** is something that is potentially dangerous or harmful, often the root cause of an unwanted outcome. Hazard is the term used to describe a natural or man-made incident that creates a risk. An example of a hazard would be overhead pipes in a file room.
- **Risk** is the potential harm that may arise from some present process or future event. Examples of risks encountered in records management include an overhead water pipe leak, a fire from faulty wiring, and unauthorized destruction of records.
- Risk management is the entire process of assessing risks, evaluating risks, and then deciding on priorities for actions and informing the agency, so that resources are available and actions can be taken to manage the risk. What we are doing in risk management for essential records entails developing a strategy to manage the risks by identifying and evaluating protection strategies appropriate for essential records. Examples of risk management include storing records in waterproof cabinets, inspecting pipes annually, and relocating records stored in risky environments.
- Risk assessment is an examination of the potential harm that may result from exposure to certain hazards. Simply put, risk assessment is the identification of risks.
  An example of risk assessment would be taking a closer look at the file room where your records are stored, and determining what harm to the records might occur if the overhead pipes in your file room leaked.

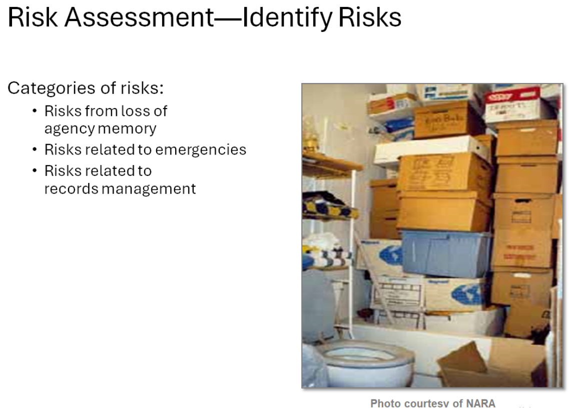
- **Risk analysis** is the systematic use of available information to determine how often specified events may occur and the magnitude of the consequences if they do occur. We use risk analysis to evaluate the *probability* of occurrence of the risk identified in the risk assessment, and the *impact* the occurrence of those risks would have on your records and information.
  For example, in your risk assessment, you determined that the overhead pipes in your file room represent a risk: they could spring a leak and damage the records. During the risk analysis, you would determine the probability of a leak's occurring and the impact it would have on the records.

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

- Identify the risks involved if the essential records remain in their current locations and on their current media
- Identify the difficulty of reconstituting the records if they are destroyed
- Determine whether off-site storage is necessary
- Determine whether use of alternative storage media is advisable
- Determine whether it is necessary to duplicate records to provide an essential record copy

Risk Assessment—Identify Risks

Slide 2-9



Risk Assessment—Identify Risks

Categories of risks:

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

Photo courtesy of NARA

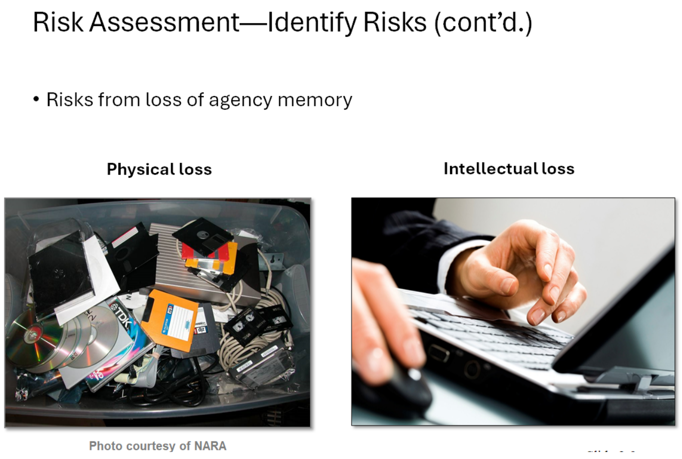
In order to identify risks properly, you must first be aware of the types of risk you may encounter. The risks relevant to an essential records program can be grouped into three categories:

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

To list all possible types of risks pertaining to essential records would be impossible. Every records management program is different and faces its own unique types of risk. The risks included in these three categories may or may not apply to your essential records program, but they should serve as a starting point to get you thinking about the risks faced by your program.

Risks From Loss of Agency Memory

Slide 2-10



Risk Assessment—Identify Risks (cont'd.)

- Risks from loss of agency memory

Physical loss
Intellectual loss

Photo courtesy of NARA

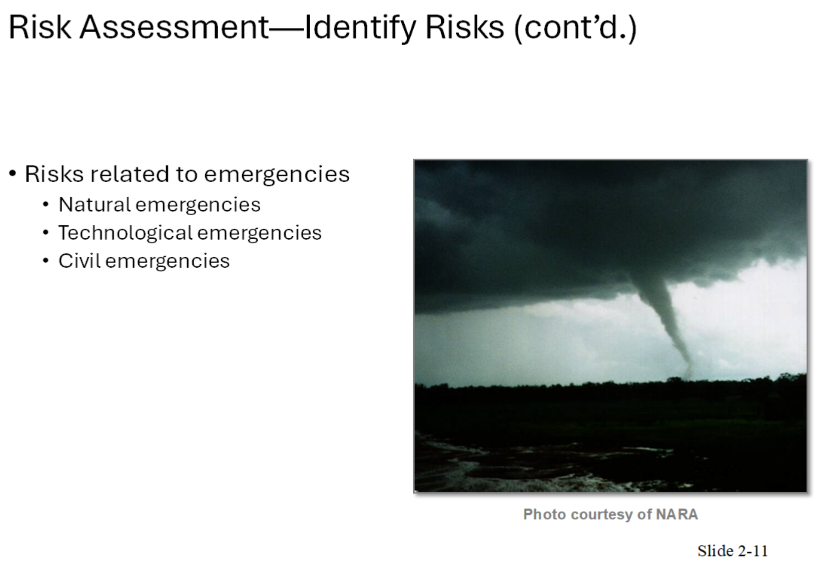
The loss of agency memory is the absence of valuable program and/or administrative information (background information, current data, and/or historical references)—an absence or lack that can result in poor decisions, incorrect information given to residents, and the loss of a historical record.

There are two types of agency memory loss:

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

Risks Related to Emergencies

Slide 2-11



Risk Assessment—Identify Risks (cont'd.)

- Risks related to emergencies
  - Natural emergencies
  - Technological emergencies
  - Civil emergencies

Photo courtesy of NARA

Slide 2-11

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

Records emergencies can be categorized as follows:

- Natural emergencies
- Technological emergencies
- Civil emergencies

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

Natural Emergencies

- Earthquakes
- Hurricanes
- Tornadoes
- Floods

Technological Emergencies

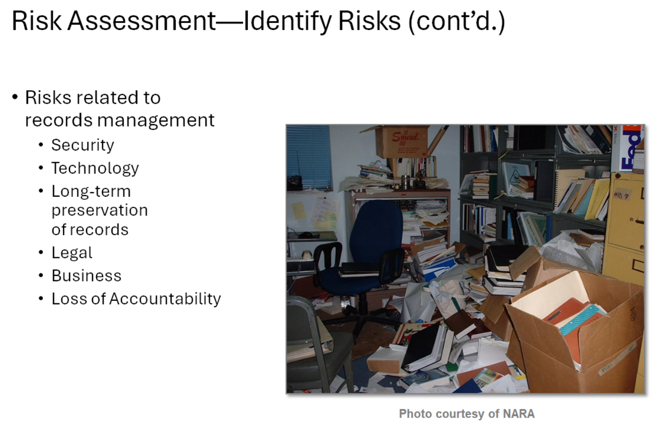
- Building and equipment failures
- Electrical malfunctions
- Hazardous material accidents
- Airplane crashes

Civil Emergencies

- Arson
- Widespread theft and looting
- Vandalism
- Terrorism
- War

Risks Related to Records Management

Slide 2-13



Risk Assessment—Identify Risks (cont'd.)

- Risks related to records management
  - Security
  - Technology
  - Long-term preservation of records
  - Legal
  - Business
  - Loss of Accountability

Photo courtesy of NARA

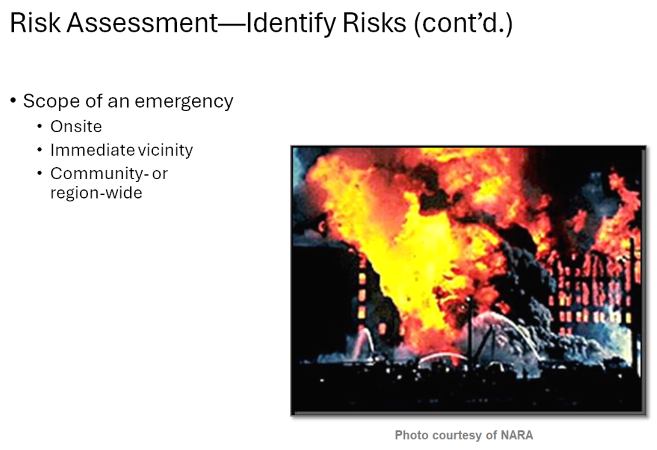
There are several types of risks related to records management:

- **Security**—Inadequate physical and network security measures increase the risk of loss or alteration of records. Also, there is a risk of restricted information, such as confidential or Privacy Act information, being released inappropriately.
- **Technology**—Risk of losing data or not being able to access data, due to changes in technology.
  - Records stored on individual hard drives are not backed up with the network, so if the hard drive crashes, the records could be lost irretrievably.
  - Technological obsolescence—Rapid changes in hardware and software formats and media put records at risk, because the agency might not be able to open and read records in the future.
- **Long-term preservation** of records:
  - Environment—Environmental conditions such as excessive heat, humidity, sunlight, etc., increase the risk that the physical media on which the records are stored will deteriorate.
  - Physical format deterioration—The longer records are kept, the greater the risk of records being lost because the physical format degrades over time, because of inherent instability in media such as floppy disks, factors like acid in paper, etc.

- **Legal—**Risk of losing a legal challenge because the agency may not have created or maintained records necessary to prove its case. Poor management of records may make the agency unable to respond to a request for access under legal discovery, the Freedom of Information Act, open records, or right-to-know laws. Retaining many records for long periods increases the number of records that an agency must sort through in response to such requests.
- **Business**—Risk of bad decision-making without necessary records, and of the poor organization of records hindering daily operations, rendering the program ineffective.
- **Accountability**—Risk of not being able to satisfy public scrutiny, of not being able to provide full government accountability, and of not being able to respond to requests for access to restricted records, because records are not created or maintained appropriately.

Scope of an Emergency or Disaster

Slide 2-14



Risk Assessment—Identify Risks (cont'd.)

- Scope of an emergency
  - Onsite
  - Immediate vicinity
  - Community- or region-wide

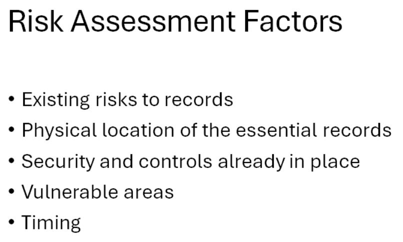
Photo courtesy of NARA

The scope of a disaster or emergency is also an important factor to consider when identifying risks. The scope can be either:

- **On site**—Events with a very narrow scope, striking only a single building, floor, or office. Use of community and organizational resources is possible. Response and recovery can begin quickly. Examples include fires, burst water pipes, or power failures.
- **Immediate vicinity**—Events in which loss of life, power outages, and massive destruction may occur, but communication and emergency services are typically not affected. Typically, backup procedures can be applied immediately, but records salvage may be hindered. Examples include tornadoes or bombing incidents.
- **Community- or region-wide**—Events with immediate disruption of communications and emergency services, power outages, and widespread destruction. Employees' homes and families are often endangered. Access to and restoration of backup information is often hindered. Getting to facilities and work sites to begin records and information recovery can be difficult. Examples include hurricanes and other widespread natural emergencies.

Risk Assessment Factors

Slide 2-15



Risk Assessment Factors

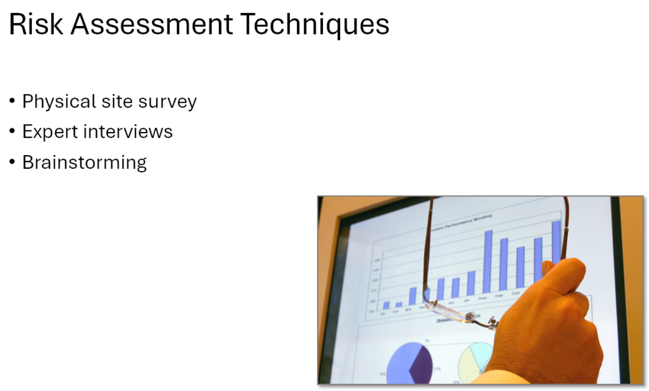
- Existing risks to records
- Physical location of the essential records
- Security and controls already in place
- Vulnerable areas
- Timing

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

- **Existing risks to records**—Are any of your agency's essential records already at risk? Are the records stored under appropriate security and environmental conditions? Will the technology you need to access and read the records be available? Are any of the records in a format that is difficult to duplicate and secure off site?
- **Physical location of the essential records**—Consider your site's physical location and characteristics. What is the building like? Is it located in a high-traffic area, a flood plain, or near other hazardous sites? Is it prone to any locality-specific risks, such as certain weather events? Are the records stored in a basement or an attic?
- **Security and controls already in place**—What security and access controls are already in place? Consider not just the controls related to securing your building and storage areas (e.g., locks, fire detection), but also security and access controls for electronic systems.
- **Vulnerable areas**—As you assess the current situation for your agency, identify the vulnerable areas that need to be addressed to minimize risk.
- **Timing**—It can also be worthwhile to examine how the risks differ, depending on whether an incident occurs during working hours or non-working hours. Agencies may assume that they'll have sufficient personnel available to respond to an incident during working hours, but what if an incident occurs during non-working hours? Will they still have sufficient personnel available to respond?

Risk Assessment Techniques

Slide 2-16



Risk Assessment Techniques

- Physical site survey
- Expert interviews
- Brainstorming

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

- Physical site survey
- Expert interviews
- Brainstorming

Physical Site Survey

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

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

- Number and types of employees who have access to the essential records
- Proximity of storage areas to laboratories, factories, or other facilities that contain flammable materials or hazardous substances
- Vulnerability to water damage

- Availability of fire control apparatus (detection, suppression, etc.) and fire department services
- Ability to reconstruct recorded information through backup procedures or use of other media

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

Expert Interviews

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

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

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

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

Brainstorming

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

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

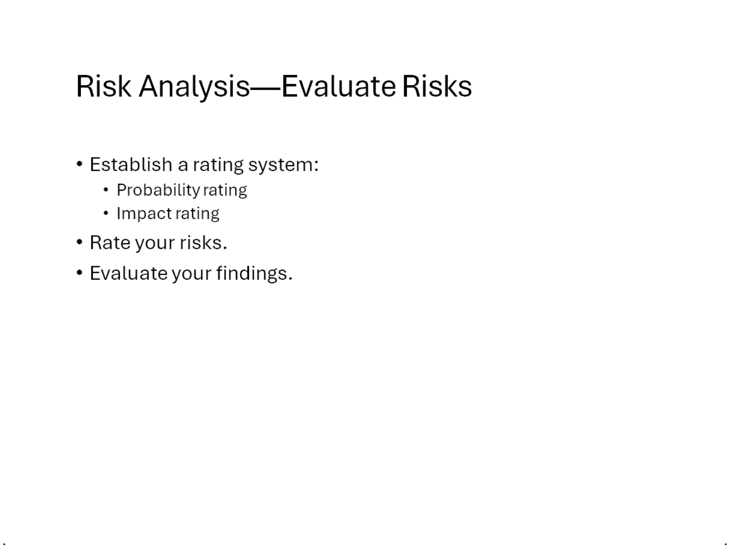
To assist with the brainstorming, expert judgments for local events can be found on websites, including those of NOAA (National Oceanic and Atmospheric Administration), USGS (U.S. Geological Survey), and DHS/FEMA, for the United States. In general, hazards from natural phenomena are ranked by state,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

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

Refer to the Council of State Archivists (CoSA) Resource Center, located at *http://www.statearchivists.org/resource-center* for resources on identifying risks.

Risk Analysis—Evaluate Risks

Slide 2-17



Risk Analysis—Evaluate Risks

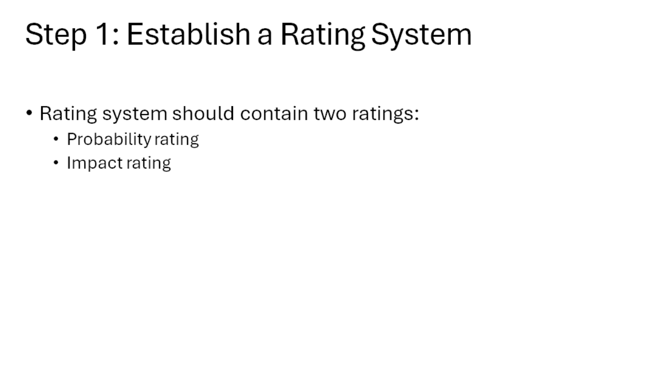
- Establish a rating system:
  - Probability rating
  - Impact rating
- Rate your risks.
- Evaluate your findings.

Once you’ve identified the risks to your essential records, your next step is to evaluate those risks by performing a risk analysis. As mentioned earlier, risk analysis evaluates the probability and the impact of identified risks. The purpose of the risk analysis is to identify where and how to direct your efforts and resources. Smaller agencies should review the options presented here and adapt them to their own needs. Some form of risk evaluation is very important.

A risk analysis consists of three steps:

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

Slide 2-18



Step 1: Establish a Rating System

- Rating system should contain two ratings:
  - Probability rating
  - Impact rating

Step 1: Establish Your Rating System

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

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

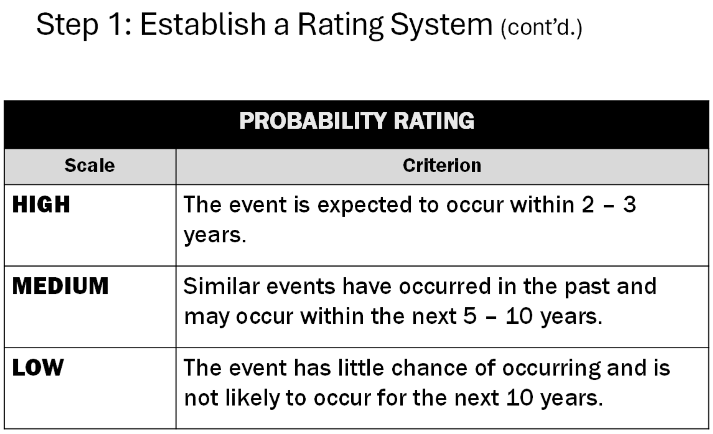
Therefore, your rating system should contain two ratings:

- A probability rating
- An impact rating

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

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

Slide 2-19



Step 1: Establish a Rating System (cont'd.)

PROBABILITY RATING	
Scale	**Criterion**
HIGH	The event is expected to occur within 2 – 3 years.
MEDIUM	Similar events have occurred in the past and may occur within the next 5 – 10 years.
LOW	The event has little chance of occurring and is not likely to occur for the next 10 years.

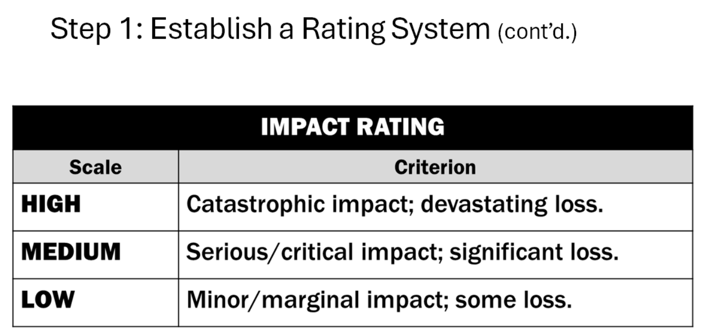
Probability Rating

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

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

Thus, you are not only deciding on a rating system, you are also deciding on a standard for what your ratings mean.

Slide 2-20



Step 1: Establish a Rating System (cont'd.)

IMPACT RATING	
Scale	**Criterion**
HIGH	Catastrophic impact; devastating loss.
MEDIUM	Serious/critical impact; significant loss.
LOW	Minor/marginal impact; some loss.

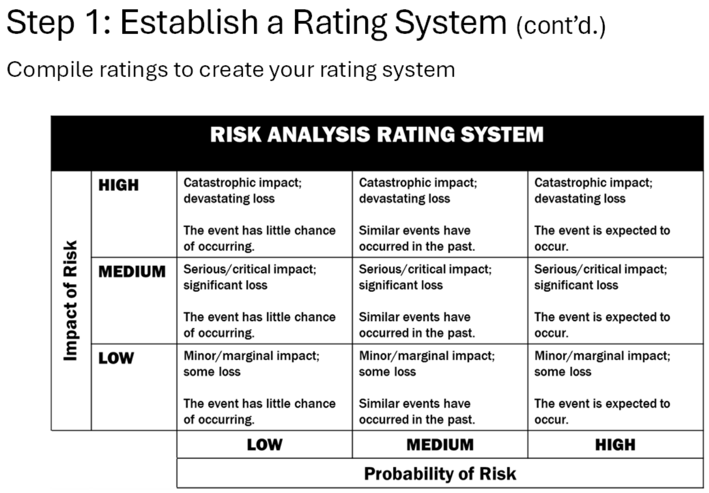
Impact Rating

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

Base your criteria on the financial and program implications of the risk event, such as:

- The cost to reconstruct lost or damaged records
- The probability of compromising an agency's program objectives
- The possibility of generating a lawsuit

Slide 2-21



Step 1: Establish a Rating System (cont'd.)

Compile ratings to create your rating system

RISK ANALYSIS RATING SYSTEM

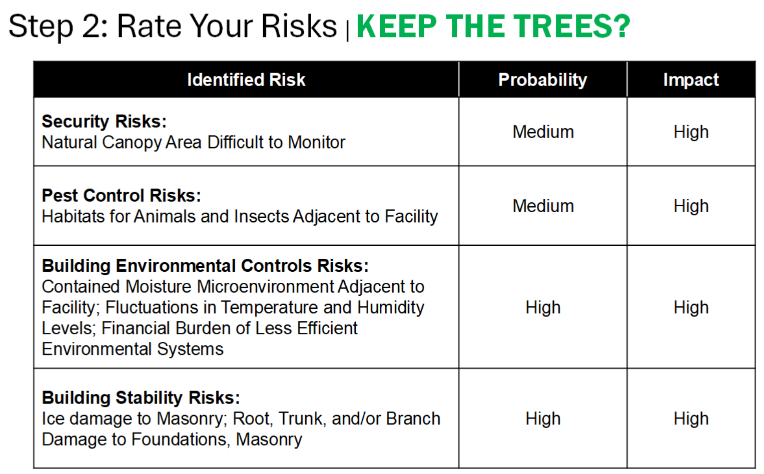
Impact of Risk	HIGH	Catastrophic impact; devastating loss The event has little chance of occurring.	Catastrophic impact; devastating loss Similar events have occurred in the past.	Catastrophic impact; devastating loss The event is expected to occur.
	MEDIUM	Serious/critical impact; significant loss The event has little chance of occurring.	Serious/critical impact; significant loss Similar events have occurred in the past.	Serious/critical impact; significant loss The event is expected to occur.
	LOW	Minor/marginal impact; some loss The event has little chance of occurring.	Minor/marginal impact; some loss Similar events have occurred in the past.	Minor/marginal impact; some loss The event is expected to occur.
		LOW	MEDIUM	HIGH
		Probability of Risk		

Step 1: Establish a Rating System

Rating System

Once you've established your rating scales, compile the scales into a single table to create your rating system. A sample rating system is provided on the next page.

Slide 2-23



Step 2: Rate Your Risks | **KEEP THE TREES?**

Identified Risk	Probability	Impact
Security Risks: Natural Canopy Area Difficult to Monitor	Medium	High
Pest Control Risks: Habitats for Animals and Insects Adjacent to Facility	Medium	High
Building Environmental Controls Risks: Contained Moisture Microenvironment Adjacent to Facility; Fluctuations in Temperature and Humidity Levels; Financial Burden of Less Efficient Environmental Systems	High	High
Building Stability Risks: Ice damage to Masonry; Root, Trunk, and/or Branch Damage to Foundations, Masonry	High	High

Step 2: Rate Your Risks

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

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

Example:

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

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

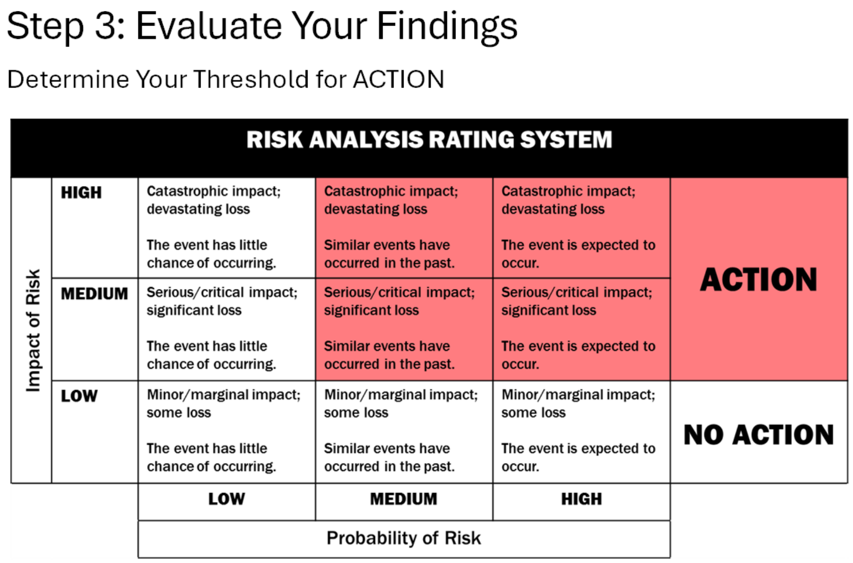
1. Debris blocking access to cabinets
2. Debris and water from storm
3. Mold and mildew
4. Temperature and humidity—unstable environment
5. Loss of data
6. Fire damage
7. Inability to access data
8. Inability to communicate

Table: Example—Rating Your Risks

IDENTIFIED RISK	PROBABILITY	IMPACT
1. Debris blocking access to cabinets	High	High
2. Debris and water from storm	High	High
3. Mold and mildew	Medium	High
4. Temperature and humidity— unstable environment	Medium	Medium
5. Loss of data	Medium	High
6. Fire damage	Low	Medium
7. Inability to access data	Medium	High
8. Inability to communicate	Medium	High

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

Slide 2-24



Step 3: Evaluate Your Findings

Determine Your Threshold for ACTION

RISK ANALYSIS RATING SYSTEM

Impact of Risk	HIGH	Catastrophic impact; devastating loss The event has little chance of occurring.	Catastrophic impact; devastating loss Similar events have occurred in the past.	Catastrophic impact; devastating loss The event is expected to occur.	ACTION
	MEDIUM	Serious/critical impact; significant loss The event has little chance of occurring.	Serious/critical impact; significant loss Similar events have occurred in the past.	Serious/critical impact; significant loss The event is expected to occur.	
	LOW	Minor/marginal impact; some loss The event has little chance of occurring.	Minor/marginal impact; some loss Similar events have occurred in the past.	Minor/marginal impact; some loss The event is expected to occur.	NO ACTION
		LOW	MEDIUM	HIGH	
		Probability of Risk			

Step 3: Evaluate Your Findings

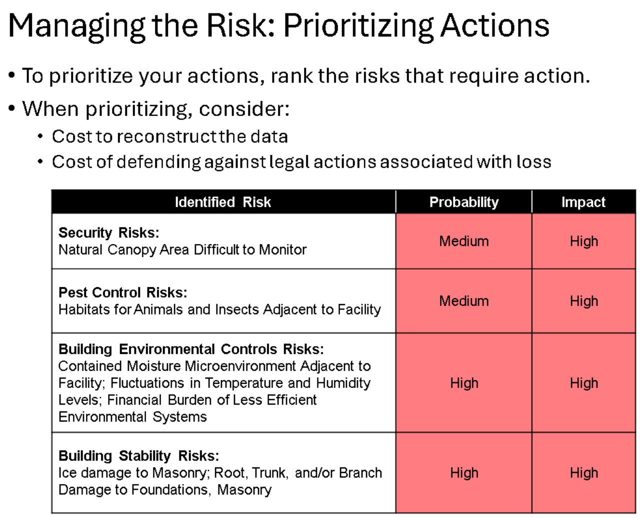
Once you’ve rated the risks to your essential records, your next step is to evaluate your findings. This evaluation will help you determine where to direct your efforts and resources for protecting your essential records.

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

Once you’ve determined your threshold for action, apply this to your risks and identify which risks require action and which do not.

Managing the Risk: Prioritizing Actions

Slide 2-25



Managing the Risk: Prioritizing Actions

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

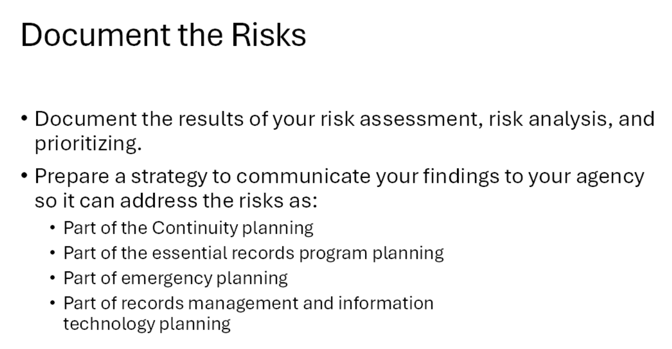
Identified Risk	Probability	Impact
Security Risks: Natural Canopy Area Difficult to Monitor	Medium	High
Pest Control Risks: Habitats for Animals and Insects Adjacent to Facility	Medium	High
Building Environmental Controls Risks: Contained Moisture Microenvironment Adjacent to Facility; Fluctuations in Temperature and Humidity Levels; Financial Burden of Less Efficient Environmental Systems	High	High
Building Stability Risks: Ice damage to Masonry; Root, Trunk, and/or Branch Damage to Foundations, Masonry	High	High

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

- The cost to reconstruct the data. This should not only include the number of staff hours involved in recreating the records if they are lost, but should also take into consideration the value of lost business, revenue, and goodwill.
- The cost of defending against legal actions associated with loss.

Document the Risks

Slide 2-26



Document the Risks

- Document the results of your risk assessment, risk analysis, and prioritizing.
- Prepare a strategy to communicate your findings to your agency so it can address the risks as:
  - Part of the Continuity planning
  - Part of the essential records program planning
  - Part of emergency planning
  - Part of records management and information technology planning

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

Include the following information in your documentation:

- Potential risk—List the risk itself. For example, the agency might face a risk of water damage to its records.
- Source of risk—Record the potential source(s) of the risk. For example, the water damage might be caused by a leaky roof.
- Location of impact—Record where the risk will have an impact. Agency-wide? One particular part of the building? One work process or function? One system?
- How probable is an incident?—Rate the probability of the risk occurring. For example, in a rainy area, the likelihood of a roof leak that damages the records might be greater, and therefore have a higher rating, than in a desert area.

- Potential effects on essential records—List the potential effects of the risk on your essential records. For example, mold and mildew might begin to grow on waterlogged records.
- Severity of impact—Rank the severity of the impact to the records, if the effect were to occur.
- Existing control measures—Record any current steps, processes, or strategies your agency has in place to detect the presence of a risk, prevent it from happening, and/or mitigate its effect.

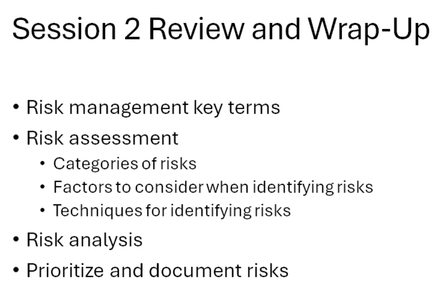
Be sure also to include the rating system used in your risk analysis, so your readers will understand what the ratings mean.

NOTE: The risk matrix that you'll prepare in this session's activity is one example of how to document the process and use it to compile a list of recommended actions, which in turn will assist the agency in planning for an essential records program and identifying the resources it will need.

Session 2 Review and Wrap-Up

Session Review

Slide 2-27



Session 2 Review and Wrap-Up

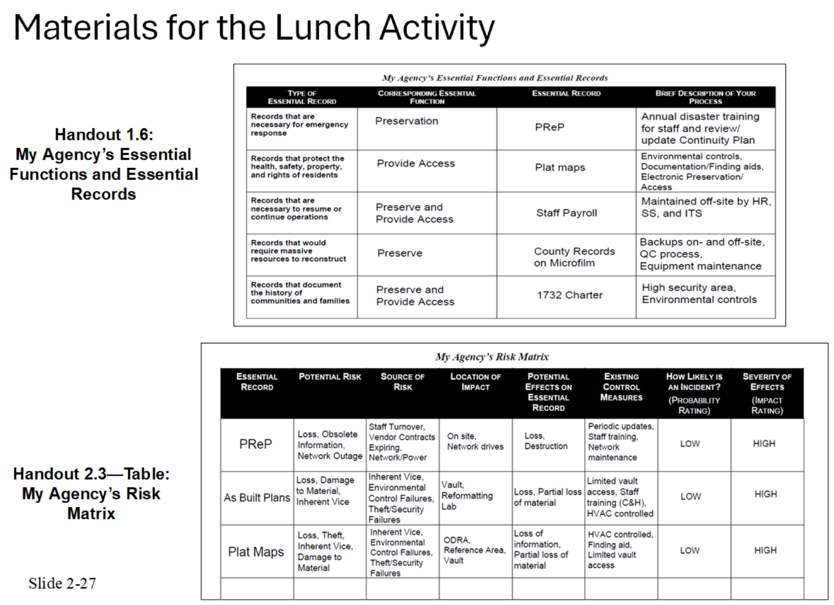
- Risk management key terms
- Risk assessment
  - Categories of risks
  - Factors to consider when identifying risks
  - Techniques for identifying risks
- Risk analysis
- Prioritize and document risks

In Session 2, you learned:

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

Activity: Identify and Evaluate Risks

Slide 2-28



Materials for the Lunch Activity

Handout 1.6: My Agency's Essential Functions and Essential Records

My Agency's Essential Functions and Essential Records

Type of Essential Record	Corresponding Essential Function	Essential Record	Brief Description of Your Process
Records that are necessary for emergency response	Preservation	PReP	Annual disaster training for staff and review/ update Continuity Plan
Records that protect the health, safety, property, and rights of residents	Provide Access	Plat maps	Environmental controls, Documentation/Finding aids, Electronic Preservation/ Access
Records that are necessary to resume or continue operations	Preserve and Provide Access	Staff Payroll	Maintained off-site by HR, SS, and ITS
Records that would require massive resources to reconstruct	Preserve	County Records on Microfilm	Backups on- and off-site, QC process, Equipment maintenance
Records that document the history of communities and families	Preserve and Provide Access	1732 Charter	High security area, Environmental controls

Handout 2.3—Table: My Agency's Risk Matrix

My Agency's Risk Matrix

Essential Record	Potential Risk	Source of Risk	Location of Impact	Potential Effects on Essential Record	Existing Control Measures	How Likely is an Incident? (Probability Rating)	Severity of Effects (Impact Rating)
PReP	Loss, Obsolete Information, Network Outage	Staff Turnover, Vendor Contracts Expiring, Network/Power	On site, Network drives	Loss, Destruction	Periodic updates, Staff training, Network maintenance	LOW	HIGH
As Built Plans	Loss, Damage to Material, Inherent Vice	Inherent Vice, Environmental Control Failures, Theft/Security Failures	Vault, Reformatting Lab	Loss, Partial loss of material	Limited vault access, Staff training (C&H), HVAC controlled	LOW	HIGH
Plat Maps	Loss, Theft, Inherent Vice, Damage to Material	Inherent Vice, Environmental Control Failures, Theft/Security Failures	ODRA, Reference Area, Vault	Loss of information, Partial loss of material	HVAC controlled, Finding aid, Limited vault access	LOW	HIGH

Slide 2-27

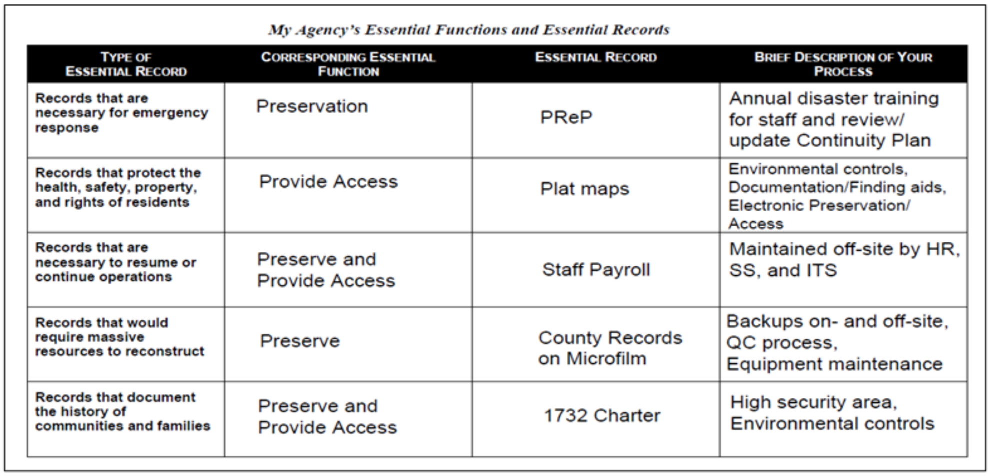
Activity materials:

- **Handout 1.6**—Determine Essential Functions and Identify Essential Records Activity
- **Handout 2.3**—Identify and Evaluate Risks Activity

Georgia Archives Example

Materials for the Lunch Activity

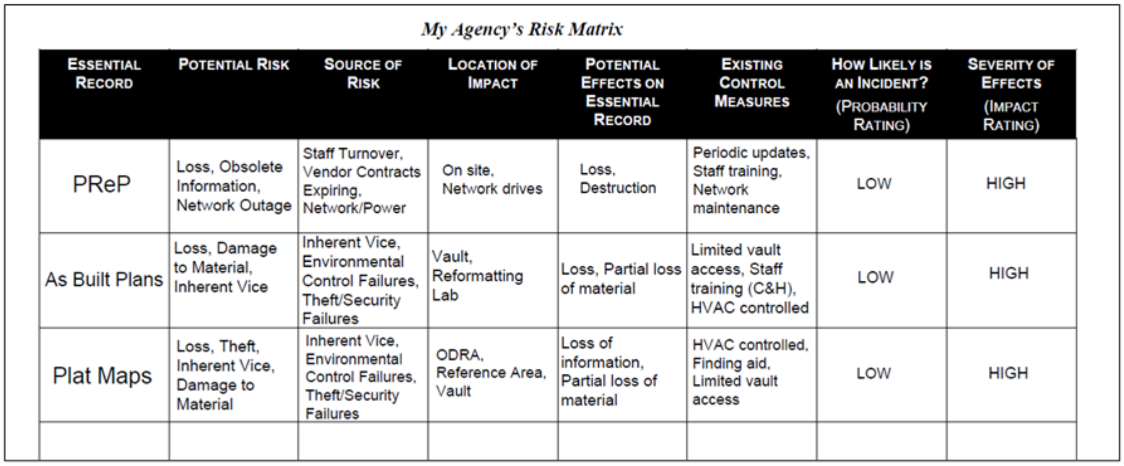
Handout 1.6: My Agency's Essential Functions and Essential Records



My Agency's Essential Functions and Essential Records

Type of Essential Record	Corresponding Essential Function	Essential Record	Brief Description of Your Process
Records that are necessary for emergency response	Preservation	PReP	Annual disaster training for staff and review/ update Continuity Plan
Records that protect the health, safety, property, and rights of residents	Provide Access	Plat maps	Environmental controls, Documentation/Finding aids, Electronic Preservation/ Access
Records that are necessary to resume or continue operations	Preserve and Provide Access	Staff Payroll	Maintained off-site by HR, SS, and ITS
Records that would require massive resources to reconstruct	Preserve	County Records on Microfilm	Backups on- and off-site, QC process, Equipment maintenance
Records that document the history of communities and families	Preserve and Provide Access	1732 Charter	High security area, Environmental controls

Handout 2.3—Table: My Agency's Risk Matrix



My Agency's Risk Matrix

Essential Record	Potential Risk	Source of Risk	Location of Impact	Potential Effects on Essential Record	Existing Control Measures	How Likely is an Incident? (Probability Rating)	Severity of Effects (Impact Rating)
PReP	Loss, Obsolete Information, Network Outage	Staff Turnover, Vendor Contracts Expiring, Network/Power	On site, Network drives	Loss, Destruction	Periodic updates, Staff training, Network maintenance	LOW	HIGH
As Built Plans	Loss, Damage to Material, Inherent Vice	Inherent Vice, Environmental Control Failures, Theft/Security Failures	Vault, Reformatting Lab	Loss, Partial loss of material	Limited vault access, Staff training (C&H), HVAC controlled	LOW	HIGH
Plat Maps	Loss, Theft, Inherent Vice, Damage to Material	Inherent Vice, Environmental Control Failures, Theft/Security Failures	ODRA, Reference Area, Vault	Loss of information, Partial loss of material	HVAC controlled, Finding aid, Limited vault access	LOW	HIGH

[This page intentionally left blank.]

Georgia Archives Essential Records Course

Session 3

Participant Guide

2024

Table of Contents

[This page intentionally left blank.]

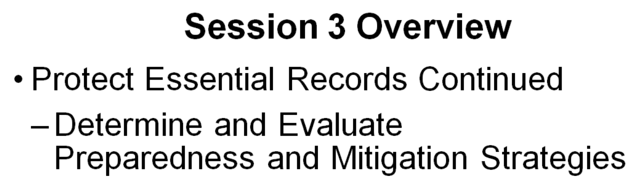
Session 3 Introduction

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**—Determine Essential Functions and Identify Essential Records Activity
  - **Handout 2.3**—Identify and Evaluate Risks Activity, with Tables 1 and 3 completed

Slide 3-3

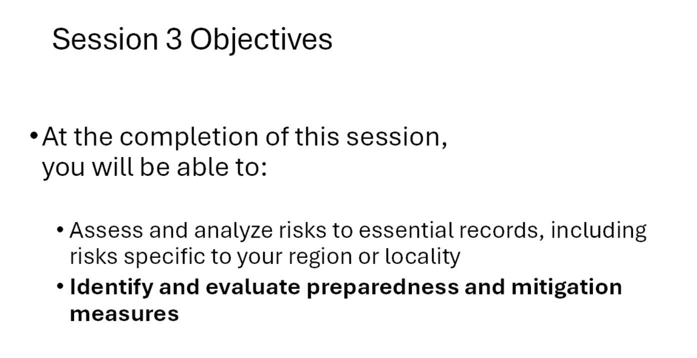


Session 3 Overview

- Protect Essential Records Continued
  - Determine and Evaluate Preparedness and Mitigation Strategies

Session 3 Objectives

Slide 3-5



Session 3 Objectives

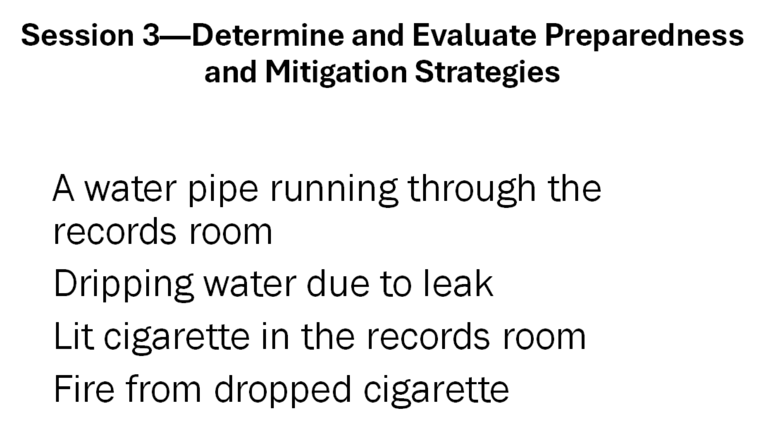
- At the completion of this session, you will be able to:
  - Assess and analyze risks to essential records, including risks specific to your region or locality
  - **Identify and evaluate preparedness and mitigation measures**

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

- **Identify and evaluate preparedness and mitigation measures**

Determine and Evaluate Preparedness and Mitigation Strategies

Slide 3-6



Session 3—Determine and Evaluate Preparedness and Mitigation Strategies

A water pipe running through the records room

Dripping water due to leak

Lit cigarette in the records room

Fire from dropped cigarette

The two **RISKS** shown on the slide are the **dripping water due to a leak** and **fire from the dropped cigarette**. The other two are the HAZARDS.

Hazards create risks. A risk to your records is that they will GET wet or that they will burn. A hazard is the thing — the leaking water pipe or lit cigarette — that creates the risk.

Strategies for Handling Risk

Slide 3-8

Strategies for Handling Risk

- Acceptance
- Mitigation

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 “make a note of it” 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. 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 probability (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.

Mitigation Measure - Records Management

Implementation of sound records management practices agency-wide provides a measure of security against potential threats and is the first type of mitigation measures. 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 3-9

Preparedness and Mitigation Measures

- Records Management
- Dispersal
- On-site protection
- Evacuation
- Backup
- Data replication
- Mirroring

www.georgiaarchives.org

Some states or localities have guidelines and regulations regarding protection of essential records. This varies widely from state to state. Check the Council of State Archivists (CoSA) Resource Center for additional information on your state. *http://www.statearchivists.org/resource-center*

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:

- Records Management
- Dispersal
- On-site protection
- Evacuation
- 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 a Continuity Plan or Continuity of Operations Plan (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

Backup

Backup can take extended periods of time for creation and for recovery (i.e., retrieving backups 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).

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 doing a separate backup of these records) or virtually (by indexing them in such a way that they can be located rapidly.

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.

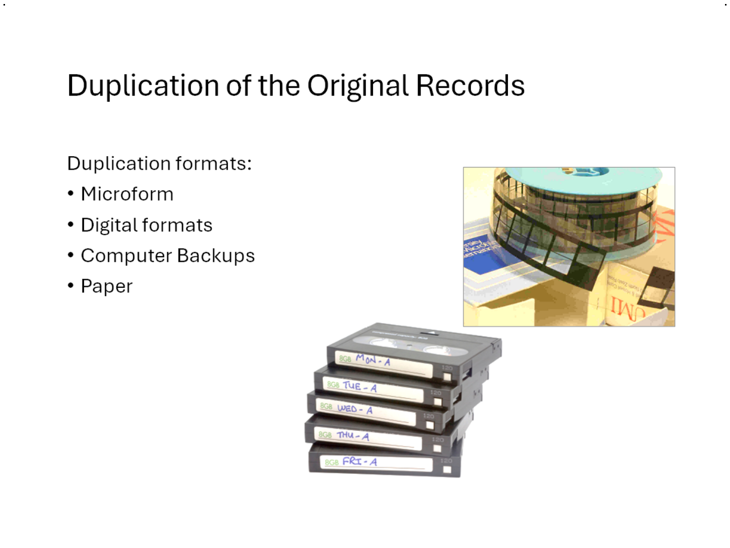
Mirroring

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 Federal Information Systems,* publication SP 800-34 at: *https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final*

Duplication of the Original Records

Slide 3-10



Duplication of the Original Records

Duplication formats:

- Microform
- Digital formats
- Computer Backups
- Paper

MON - A
TUE - A
WED - A
THU - A
FRI - A

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.

- **Computer Backups**—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 backups 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 computer backup represent an appropriate option for your particular circumstances and requirements. If the backups' 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 has 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 un-manipulated image that has not been dodged (lightening a spot), burned (contrast raised to high), 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)

If you've heard of the Federal Agencies Digital Guidelines Initiative (FADGI), which is the federal standards for digitization and reformatting, and are concerned, this does not apply to State records. If you're curious about FADGI, more information can be found at *https://www.digitizationguidelines.gov/*

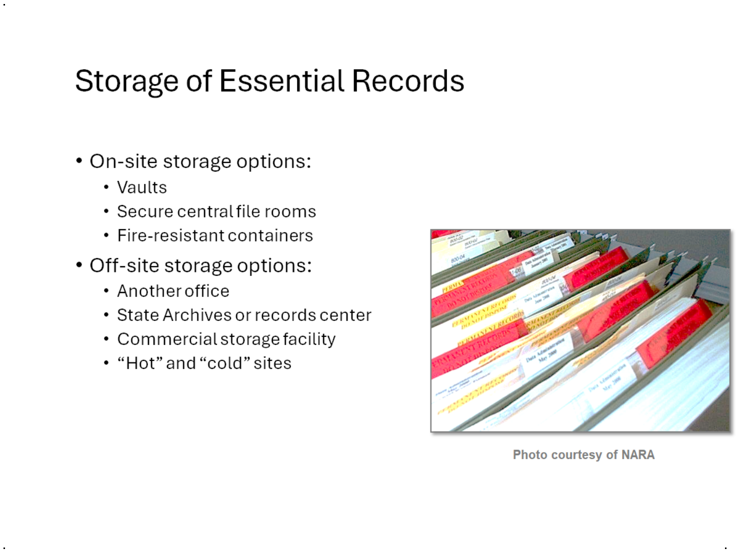
Retention of Backup Copies

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 3-11



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

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.

OCGA 50-18-94(5)

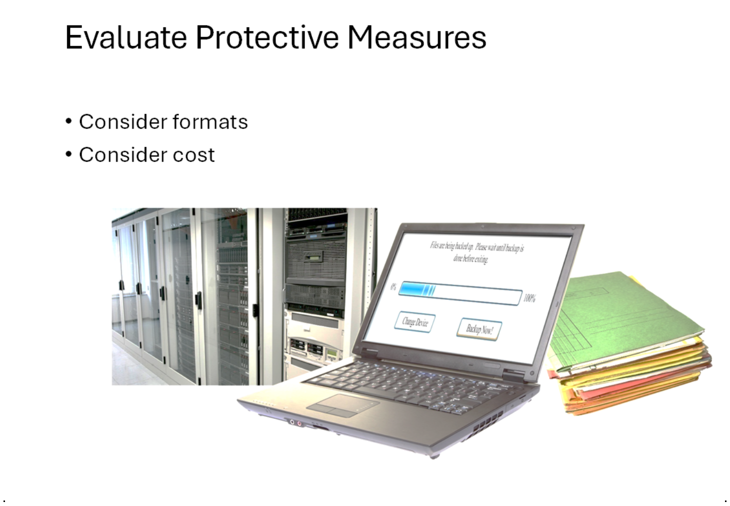
"Submit to the division, in accordance with the rules and regulations of the division, a recommended retention schedule for each record series in its custody, except that schedules for common-type files may be established by the division. No records will be scheduled for permanent retention in an office. No records will be scheduled for retention any longer than is absolutely necessary in the performance of required functions. Records requiring retention for several years will be transferred to the records center for low-cost storage at the earliest possible date following creation."

OCGA 36-9-5(c)(2)(D)

"At a location not more than 100 miles from the county in a data storage and retrieval facility approved by the county governing authority within the State of Georgia which is in a building or facility which is in compliance with the fire safety standards applicable to archives and record centers as established by the National Fire Protection Association in Standard No. 232, as such standard was adopted on August 11, 1995. If documents are stored outside the county where the documents were created, the government entity shall bear all costs of transporting such documents back to the county of origin for purposes of responding to requests under Article 4 of Chapter 18 of Title 50, relating to inspections of public records."

Evaluate Protective Measures

Slide 3-12



Evaluate Protective Measures

- Consider formats
- Consider cost

Files are being backed up. Please wait until backup is done before exiting.
0%
100%
Change Device
Backup Now!

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

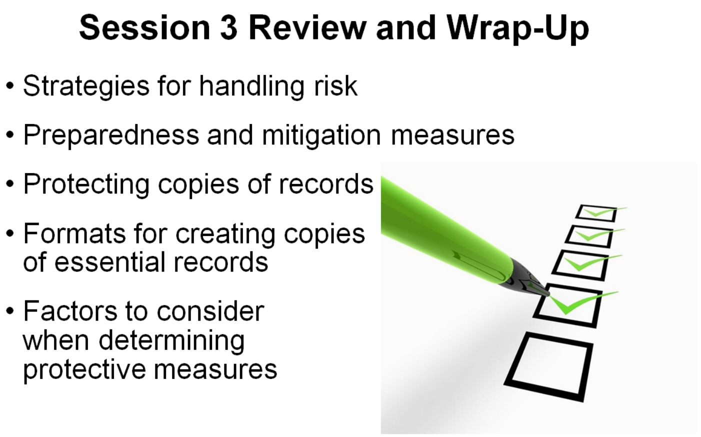
The cost of protecting essential records will require a long-term commitment from management. Management must be able to weigh the cost of protecting the records against the risk of not recovering the records in the event of an emergency or disaster.

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.

Session 3 Review and Wrap-Up

Session Review

Slide 3-13



Session 3 Review and Wrap-Up

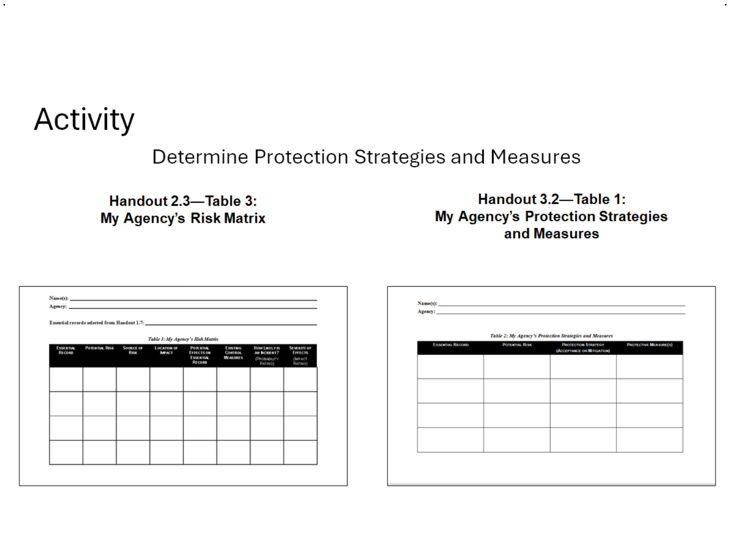
- Strategies for handling risk
- Preparedness and mitigation measures
- Protecting copies of records
- Formats for creating copies of essential records
- Factors to consider when determining protective measures

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 3-14



Activity

Determine Protection Strategies and Measures

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

Name(s): ____________________
Agency: ____________________

Essential records selected from Handout 1.7: ____________________

Table 3: My Agency's Risk Matrix

Essential Record	Potential Risk	Source of Risk	Location of Impact	Potential Effects on Essential Record	Existing Control Measures	How Likely is an Incident? (Probability Rating)	Severity of Effects (Impact Rating)

Handout 3.2—Table 1:
My Agency's Protection Strategies
and Measures

Name(s): ____________________
Agency: ____________________

Table 2: My Agency's Protection Strategies and Measures

Essential Record	Potential Risk	Protection Strategy (Acceptance or Mitigation)	Protective Measure(s)

Activity materials:

- **Handout 2.3**—Identify and Evaluate Risks Activity
- **Handout 3.2**—Determine Protection Strategies and Measures Activity

[This page intentionally left blank.]

Georgia Archives Essential Records Course

Session 4

Participant Guide

2024

Table of Contents

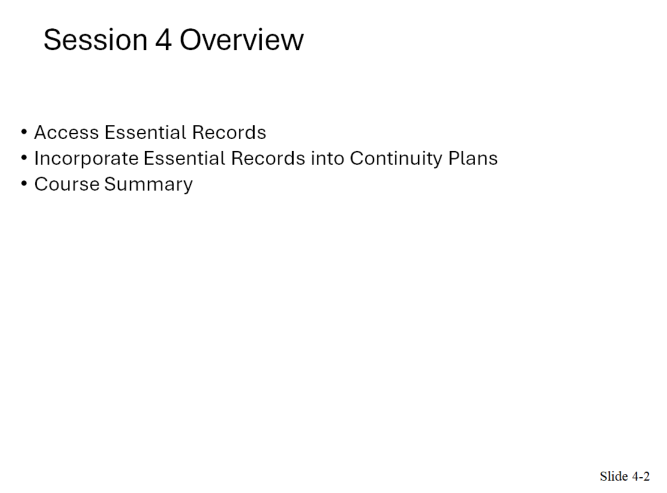
Session 4 Introduction

Session 4 Overview

Required materials for Session 4:

- Session 4 Participant Guide
- Session 4 handouts:
  - **Handout 4.1**—Access Priorities Table
  - **Handout 4.2**—Establishing a Duplication Schedule for Essential Records
  - **Handout 4.3**—Determine Timeframes for Accessibility Activity
  - **Handout 4.4**—Essential Records Template
- Materials from prior sessions:
  - **Handout 1.1**—Essential Records
  - **Handout 1.3**—Potential Candidates for Essential Records Status
  - **Handout 1.5**—Essential Records Questionnaire
  - **Handout 1.6**—Determine Essential Functions and Identify Essential Records Activity
  - **Handout 3.2**—Determine Protection Strategies and Measures Activity, with Table 1 completed

Slide 4-2



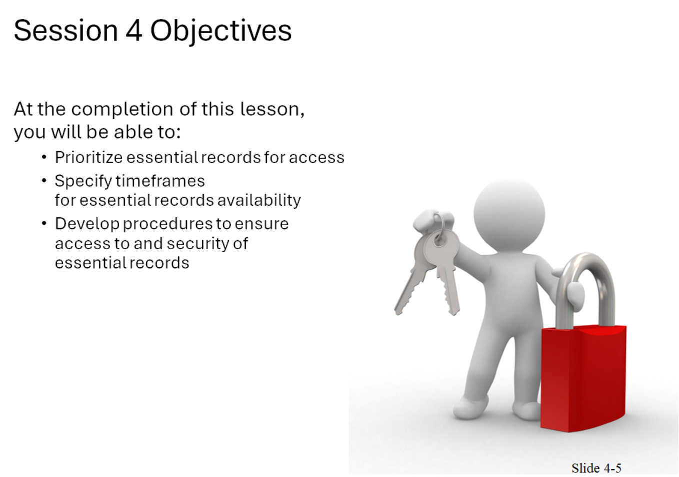
Session 4 Overview

- Access Essential Records
- Incorporate Essential Records into Continuity Plans
- Course Summary

Slide 4-2

Session 4 Objectives

Slide 4-5



Session 4 Objectives

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

- Prioritize essential records for access
- Specify timeframes for essential records availability
- Develop procedures to ensure access to and security of essential records

Slide 4-5

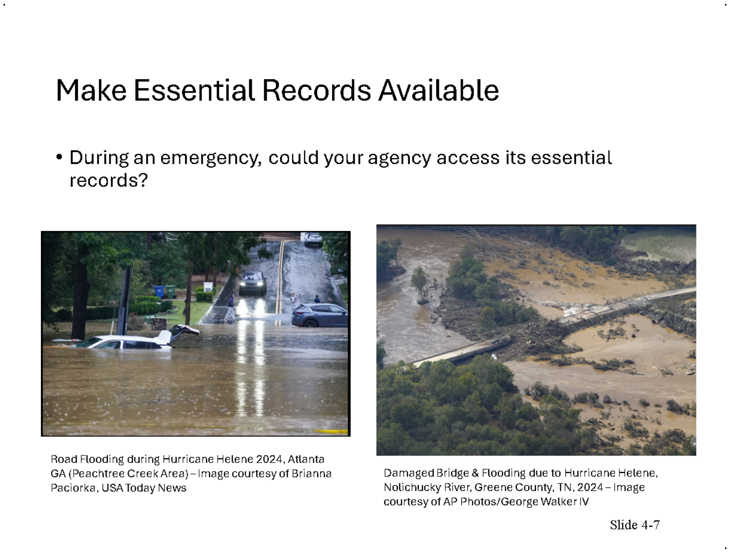
At the completion of this session, you will be able to:

- Prioritize essential records
- Specify timeframes for essential records availability
- Develop procedures to ensure access to and security of essential records

Lesson 1: Ensure Access to Essential Records

Make Essential Records Available

Slide 4-7



Make Essential Records Available

- During an emergency, could your agency access its essential records?

Road Flooding during Hurricane Helene 2024, Atlanta GA (Peachtree Creek Area) – Image courtesy of Brianna Paciorka, USA Today News

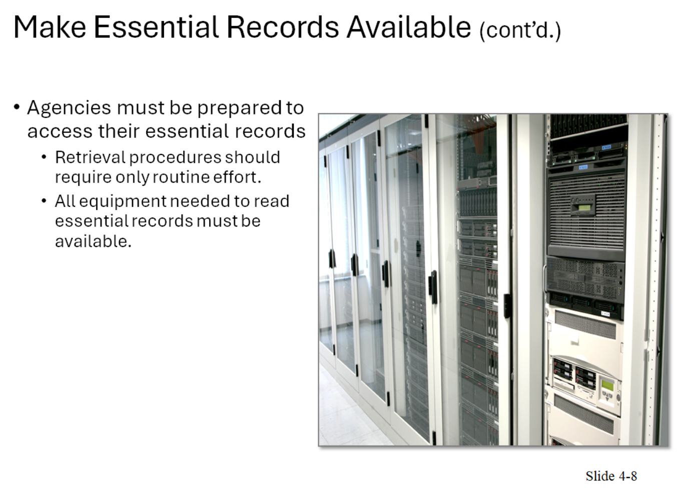
Damaged Bridge & Flooding due to Hurricane Helene, Nolichucky River, Greene County, TN, 2024 – Image courtesy of AP Photos/George Walker IV

Slide 4-7

As we know, essential government services can be interrupted by disastrous events ranging from something as small as a burst pipe to something as catastrophic as a terrorist attack. Such disruptions may last for a short time, or they may result in a complete stoppage of government operations.

In the event of an emergency, could your agency access the essential records it needs to perform its mission?

Slide 4-8



Make Essential Records Available (cont'd.)

- Agencies must be prepared to access their essential records
  - Retrieval procedures should require only routine effort.
  - All equipment needed to read essential records must be available.

Slide 4-8

Regardless of the scale of the emergency, agencies must be able to respond to the situation, continue to function and provide services to the public under emergency operating conditions, and resume normal business afterward. Essential records make this possible, so agencies must be prepared to access their essential records.

Agencies should ensure that retrieval procedures for essential records require only routine effort to locate needed information, especially since individuals unfamiliar with the records may need to use them during an emergency.

Agencies should also ensure that all equipment needed to read essential records will be available in case of emergency. For electronic records systems, agencies should also ensure that system documentation adequate to operate the system and access to the records will be available in case of emergency and that they have the keys or access codes required.

Federal Emergency Management Agency's (FEMA) *Continuity Guidance Circular 1 (CGC1)* recommends:

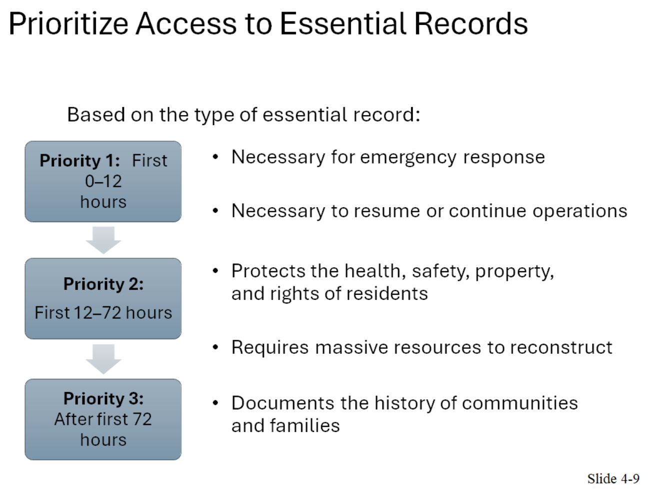
"As soon as possible after continuity of operations activation, but recommended within 12 hours of such activation, continuity personnel at the continuity facility should have access to the appropriate media for accessing vital [essential] records, such as:

a. A local area network and files,
b. Electronic versions of vital [essential] records,
c. Supporting information systems and data,
d. Internal and external email and email archives,
e. Hard copies of vital [essential] records."

Prioritize Access to Essential Records

Prioritize Based on the Type of Essential Record

Slide 4-9



Prioritize Access to Essential Records

Based on the type of essential record:

Priority 1: First 0–12 hours
- Necessary for emergency response
- Necessary to resume or continue operations

Priority 2: First 12–72 hours
- Protects the health, safety, property, and rights of residents
- Requires massive resources to reconstruct

Priority 3: After first 72 hours
- Documents the history of communities and families

Slide 4-9

During an emergency, you have limited time and resources to access your essential records, so it's important to prioritize which essential records need to be accessed when. You will have to determine which essential records are needed immediately and which essential records may not be needed for several days or even weeks. That way, you can focus your energies on accessing only the records needed at that particular time.

Access to an agency's essential records is prioritized based on the type of essential record involved.

In the first session, we identified the five types of essential records:

- Records that are necessary for emergency response
- Records that are necessary to resume or continue operations
- Records that protect the health, safety, property, and rights of residents
- Records that would require massive resources to reconstruct
- Records that document the history of communities and families

As you may recall, **Handout 1.1—Essential Records** provides an overview of the types of essential records and examples of each, and also provides prioritizing guidance.

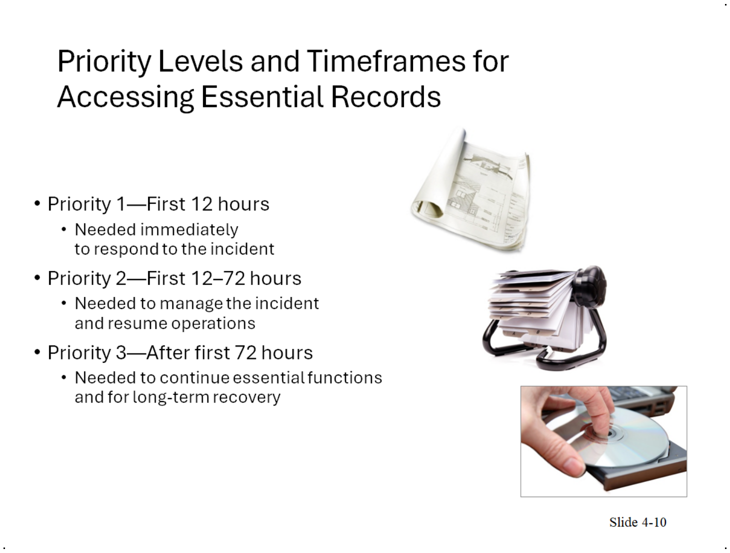
The column on the left of the table in **Handout 1.1** shows the priorities for accessing essential records. In general, the priorities for accessing essential records follow the same order as that in which the types of essential records are listed in this table.

The priorities start at the top with Priority 1, those records which are needed immediately for emergency response, and progress down to Priority 3, those records which will be needed later as the agency and community recover.

This ranking is meant to suggest only an overall pattern, not a rigidly hierarchy. Administrative responsibilities and particular circumstances will affect each agency’s approach to setting priorities. For instance, in November of an election year, voting records are likely to be of higher priority than at other times.

Priority Levels and Timeframes for Accessing Essential Records

Slide 4-10



Priority Levels and Timeframes for Accessing Essential Records

- Priority 1—First 12 hours
  - Needed immediately to respond to the incident
- Priority 2—First 12–72 hours
  - Needed to manage the incident and resume operations
- Priority 3—After first 72 hours
  - Needed to continue essential functions and for long-term recovery

Slide 4-10

Priority 1—Needed in the first 12 hours

Priority 1 essential records are the records essential for emergency operations and are therefore needed immediately—in the first few hours of a crisis or emergency—to respond to that emergency. These Priority 1 essential records may include:

- Continuity Plans
- Telephone trees
- Delegations of authority
- Security clearance rosters
- Building blueprints
- Utility maps and diagrams
- Media policy directives
- Essential records inventory lists
- Contact information for disaster recovery vendors

Priority 2—Needed in the first 12–72 hours

Records classified under Priority 2 include records that are needed to manage the incident and resume operations.

Examples include:

- Systems manuals for databases and networks
- Payroll records
- Time and attendance records
- Combination codes to restricted areas or equipment
- Combination codes and/or keys for building entry

Priority 3—Needed after the first 72 hours

Priority 3 essential records are those that would be needed to continue essential functions if normal agency records were unavailable for a prolonged period due to a catastrophic event (causing long-term displacement of personnel and equipment from the worksite to a new operating location).

These include records that are needed off site to work on specific programs or projects most critical to your agency's mission. They also include records that would take such massive resources to reconstruct that they should receive special protection against damage or destruction.

Also included among Priority 3 records are those that are needed for long-term recovery of the agency and broader community, including those that document the history of the community and its residents.

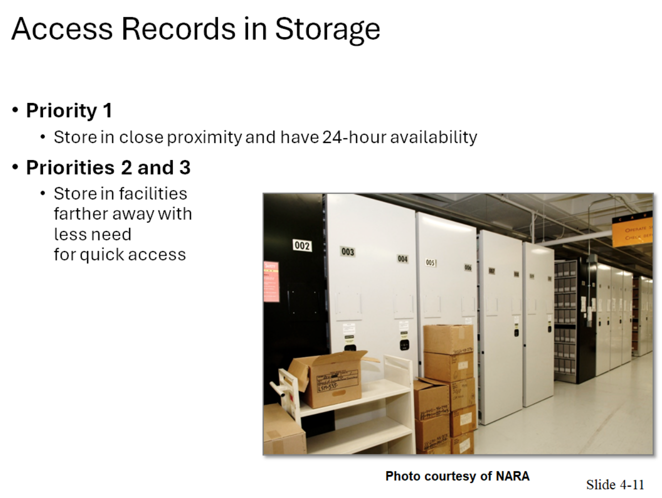
Your Stakeholders Are Resources

Some of the same stakeholders you included in identifying essential records—Agency head, mission-critical program or department heads (Information Technology [IT] Director and systems analysts, etc.)—are also important to include in setting priorities and timeframes.

If you gathered information previously using a questionnaire like the one provided in **Handout 1.5—Essential Records Questionnaire**, you will already have the basic information you need. You will already have asked, "How soon would you need access to the records (hours, days, weeks)?" Given the essential records you've identified, you should determine which stakeholders you may need to revisit.

Access Records in Storage

Slide 4-11



Access Records in Storage

- **Priority 1**
  - Store in close proximity and have 24-hour availability
- **Priorities 2 and 3**
  - Store in facilities farther away with less need for quick access

Photo courtesy of NARA

Slide 4-11

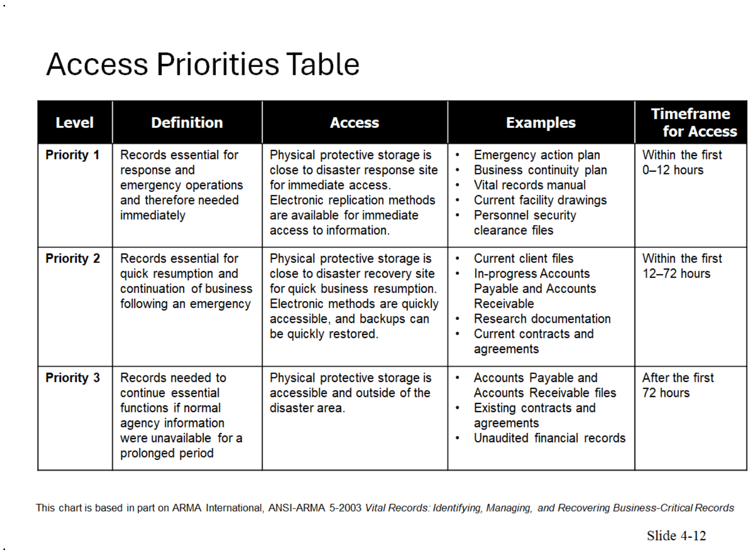
Generally, how you prioritize your essential records determines the type of storage option you select to protect them.

You need to access your Priority 1 essential records during and immediately following an emergency. Therefore, you will want to store those records in close proximity to your office and have 24-hour availability (which may mean storage at a “hot” site, and may mean storing the records in a format that does not rely on special equipment to be read).

Typically, you would not need your Priority 2 and 3 essential records as quickly as you would your Priority 1 essential records, so Priority 2 and 3 essential records could be stored in facilities farther away.

Access Priorities: Putting It All Together

Slide 4-12



Access Priorities Table

Level	Definition	Access	Examples	Timeframe for Access
Priority 1	Records essential for response and emergency operations and therefore needed immediately	Physical protective storage is close to disaster response site for immediate access. Electronic replication methods are available for immediate access to information.	• Emergency action plan • Business continuity plan • Vital records manual • Current facility drawings • Personnel security clearance files	Within the first 0–12 hours
Priority 2	Records essential for quick resumption and continuation of business following an emergency	Physical protective storage is close to disaster recovery site for quick business resumption. Electronic methods are quickly accessible, and backups can be quickly restored.	• Current client files • In-progress Accounts Payable and Accounts Receivable • Research documentation • Current contracts and agreements	Within the first 12–72 hours
Priority 3	Records needed to continue essential functions if normal agency information were unavailable for a prolonged period	Physical protective storage is accessible and outside of the disaster area.	• Accounts Payable and Accounts Receivable files • Existing contracts and agreements • Unaudited financial records	After the first 72 hours

This chart is based in part on ARMA International, ANSI-ARMA 5-2003 *Vital Records: Identifying, Managing, and Recovering Business-Critical Records*

Slide 4-12

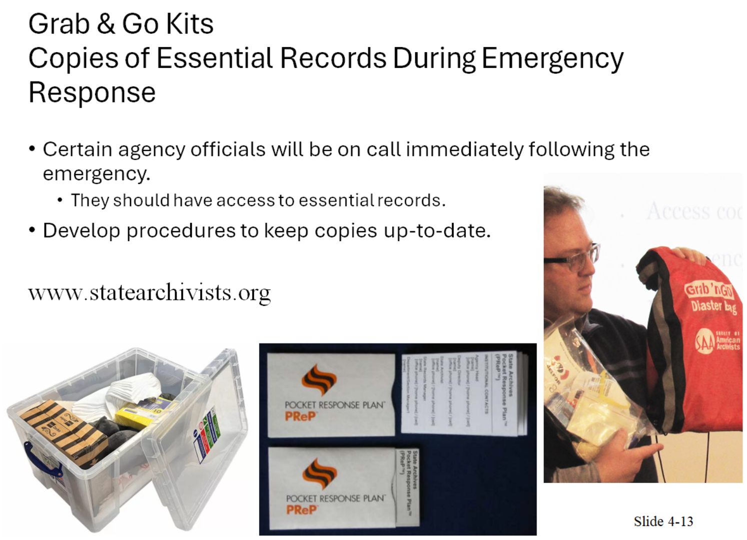
The Access Priorities Table shown on the slide and in **Handout 4.1—Access Priorities Table** summarizes the timeframe and storage considerations for each priority level.

You should assign priority levels to each of your agency's essential records. This allows both agency staff and emergency responders to identify quickly and easily which essential records should be retrieved and when. These are decisions you don't want to have to spend time making during an emergency.

Once priorities are assigned, you should develop a table based on **Handout 4.1** that could be incorporated in your agency's Continuity Plan.

“Grab and Go” Kits

Slide 4-13



Grab & Go Kits
Copies of Essential Records During Emergency Response

- Certain agency officials will be on call immediately following the emergency.
  - They should have access to essential records.
- Develop procedures to keep copies up-to-date.

www.statearchivists.org

POCKET RESPONSE PLAN
PReP
Grab 'n Go
Diaster bag

Slide 4-13

Immediately following an emergency, certain agency officials will be on call. To guarantee that these essential personnel have access to the necessary essential records, they should be provided with “Grab and Go” kits that contain copies of specific essential records.

“Grab and Go” kits should be kept by all essential personnel “on their persons” (at home or in their vehicles), and should include specific Priority 1 documents (those needed during and immediately after an emergency) and supplies (water, medical materials, etc.).

The essential records in these kits should be updated or cycled on the same schedule as all your essential records so that the kit remains current.

Development of the kits is mainly the responsibility of a safety manager or Continuity planner. However, records management can contribute to what goes into the kits.

Examples of the types of essential records and information to include in a “Grab and Go” kit are:

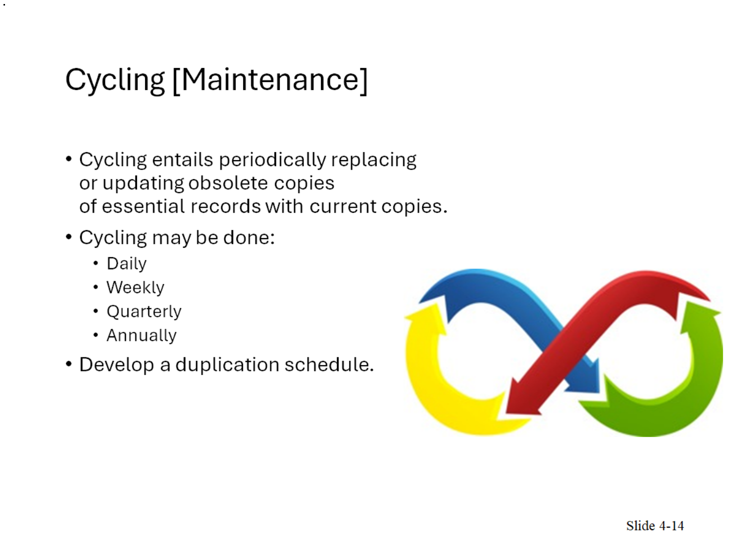
- Continuity Plan
- Delegations of authority
- Media procedures
- Emergency telephone lists

- Passwords
- Access codes
- Emergency passes
- Directions to a “hot” site
- CoSA PReP

Keep in mind that some of these documents may contain highly sensitive security information. Though they must be readily available in an emergency, you must take precautions so that sensitive information does not fall into the hands of unauthorized personnel. If you store the information on an electronic device, make sure that it is password-protected.

Cycling

Slide 4-14



Cycling [Maintenance]

- Cycling entails periodically replacing or updating obsolete copies of essential records with current copies.
- Cycling may be done:
  - Daily
  - Weekly
  - Quarterly
  - Annually
- Develop a duplication schedule.

Slide 4-14

Cycling (or "maintenance") is the periodic replacement or updating of obsolete copies of essential records with current copies.

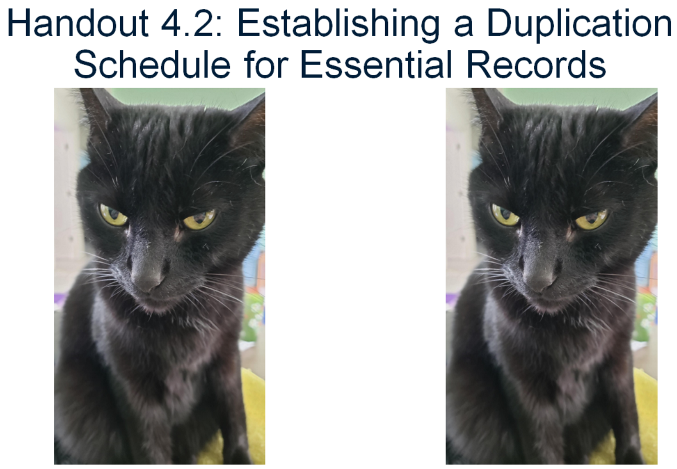
Essential records don't stay "essential" forever. Many essential records have limited time value: They are essential only for a specific period of time, and once that time has passed, the copies become valueless for post-emergency resumption of activities.

In order for the most current or up-to-date essential records to be available during an emergency, agencies must ensure that their essential records are cycled as a matter of routine. Cycling may be done on a daily, weekly, quarterly, or annual basis—depending on the content of the records, the media on which they are stored, and access priorities.

The agency is responsible for periodically cycling (updating) essential records by removing obsolete items and replacing them with the most recent versions, when necessary.

Remember, the essential record copy is typically a duplicate of the original record, and therefore may not be subject to your agency's records schedule. If that is the case, it should be destroyed or deleted when it is replaced by an updated copy.

Slide 4-15



Handout 4.2: Establishing a Duplication Schedule for Essential Records

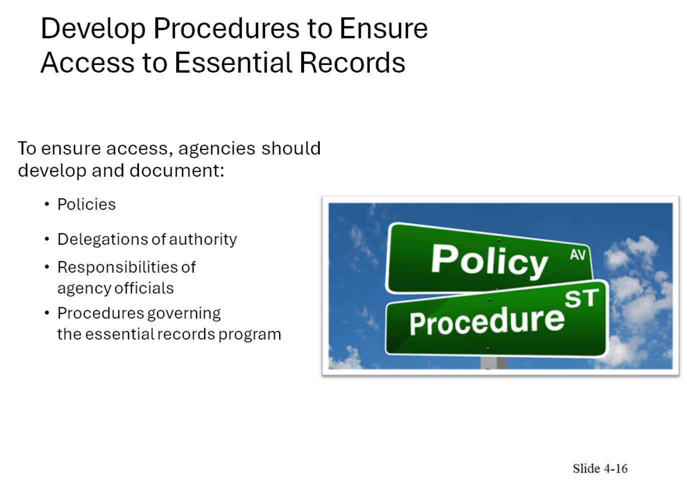
Develop a Duplication Schedule

One way to implement and track this requirement is to develop a duplication schedule or calendar. A duplication schedule simply allows you to set up cycling frequency—daily, weekly, monthly, quarterly, or annually—and to document that action formally.

Refer to **Handout 4.2—Establishing a Duplication Schedule for Essential Records** for additional guidance.

Develop Procedures to Ensure Access to Essential Records

Slide 4-16



Policy AV
Procedure ST

Develop Procedures to Ensure Access to Essential Records

To ensure access, agencies should develop and document:

- Policies
- Delegations of authority
- Responsibilities of agency officials
- Procedures governing the essential records program

Slide 4-16

Agencies must develop and document procedures for the use of essential records during an emergency.

Agencies should make responsible personnel familiar with these procedures.

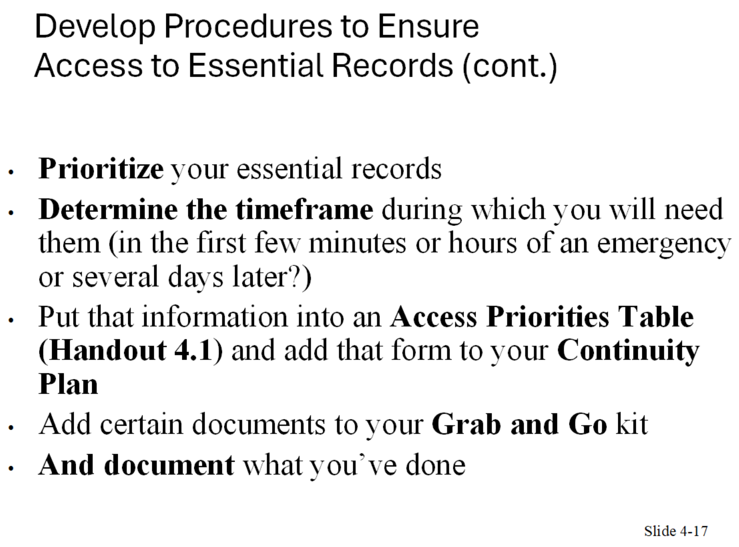
Each agency should document the following essential record information in appropriate issuances, such as directives or procedural manuals:

- Policies
- Delegations of authority
- Responsibilities of agency officials
- Procedures governing the essential records program

The issuances should clearly assign responsibility for coordinating essential records recovery plans and activities. They should also designate the members of the essential records team to be activated in time of need. Agencies should distribute this essential records information to all appropriate staff members.

Develop Procedures to Ensure Access to Essential Records (cont.)

Slide 4-17



Develop Procedures to Ensure
Access to Essential Records (cont.)

- **Prioritize** your essential records
- **Determine the timeframe** during which you will need them (in the first few minutes or hours of an emergency or several days later?)
- Put that information into an **Access Priorities Table (Handout 4.1**) and add that form to your **Continuity Plan**
- Add certain documents to your **Grab and Go** kit
- **And document** what you've done

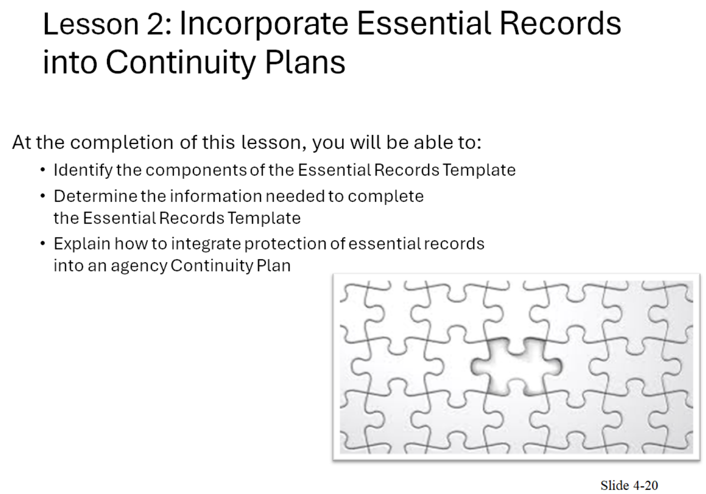
Slide 4-17

Above are the procedures for ensuring access to essential records.

Lesson 2: Incorporate Essential Records into Continuity Plans

Lesson 2 Objectives

Slide 4-20



Lesson 2: Incorporate Essential Records into Continuity Plans

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

- Identify the components of the Essential Records Template
- Determine the information needed to complete the Essential Records Template
- Explain how to integrate protection of essential records into an agency Continuity Plan

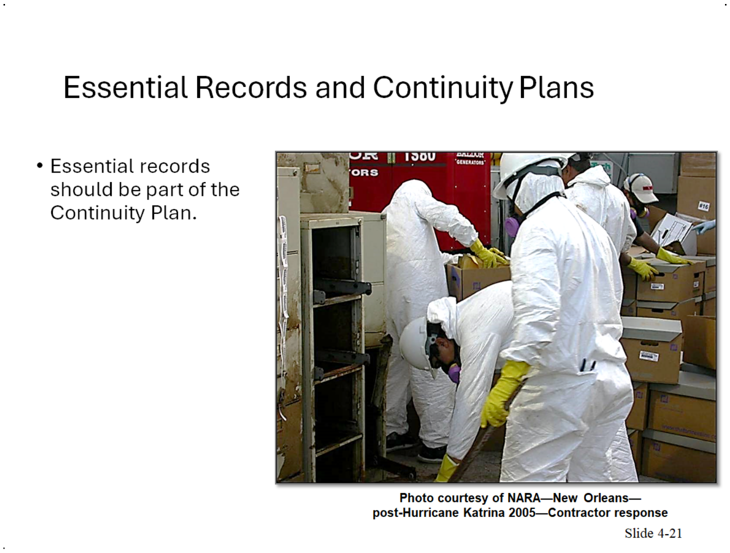
Slide 4-20

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

- Identify the components of the Essential Records Template
- Determine the information needed to complete the Essential Records Template
- Explain how to integrate protection of essential records into an agency Continuity Plan

Essential Records and Continuity Plans

Slide 4-21



Essential Records and Continuity Plans

- Essential records should be part of the Continuity Plan.

Photo courtesy of NARA—New Orleans—
post-Hurricane Katrina 2005—Contractor response

Slide 4-21

Essential records should be part of an agency's Continuity Plan, because records are critical for responding to an emergency and for continuing operations. These include the Continuity Plan itself, as well as occupant emergency plans, telephone trees, delegations of authority, security clearance rosters, building blueprints, media policy directives, and essential records inventory lists.

In addition, residents of our states and communities depend on us to keep records that are critical to protecting their health, safety, property, and rights.

Many agencies, states, and localities require essential records to be part of their Continuity Plan, but even if yours does not, operations cannot continue without essential records and it is important to include them in your Continuity Plan.

Sample Continuity Plans

Let’s take a look at some sample Continuity Plan Templates to see where and how essential records are incorporated.

Continuity Plan Example 1

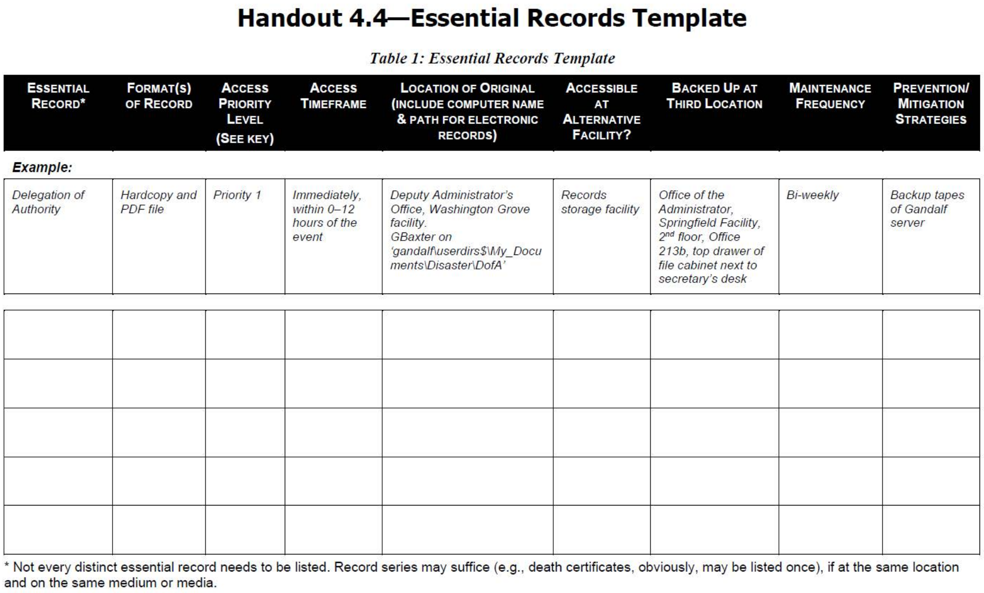
FEMA’s COOP Plan Template:
www.fema.gov/emergency-managers/national-prepardness/continuity/templates

Continuity Plan Example 2

National Institute of Standards and Technology’s (NIST) Contingency Plan Template:
http://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

Essential Records Template

Slide 4-22



Handout 4.4—Essential Records Template

Table 1: Essential Records Template

Essential Record*	Format(s) of Record	Access Priority Level (See Key)	Access Timeframe	Location of Original (Include Computer Name & Path for Electronic Records)	Accessible at Alternative Facility?	Backed Up at Third Location	Maintenance Frequency	Prevention/ Mitigation Strategies
Example:								
Delegation of Authority	*Hardcopy and PDF file*	*Priority 1*	*Immediately, within 0–12 hours of the event*	*Deputy Administrator's Office, Washington Grove facility.* *GBaxter on 'gandalf\userdirs$\My_Documents\Disaster\DofA'*	*Records storage facility*	*Office of the Administrator, Springfield Facility, 2nd floor, Office 213b, top drawer of file cabinet next to secretary's desk*	*Bi-weekly*	*Backup tapes of Gandalf server*

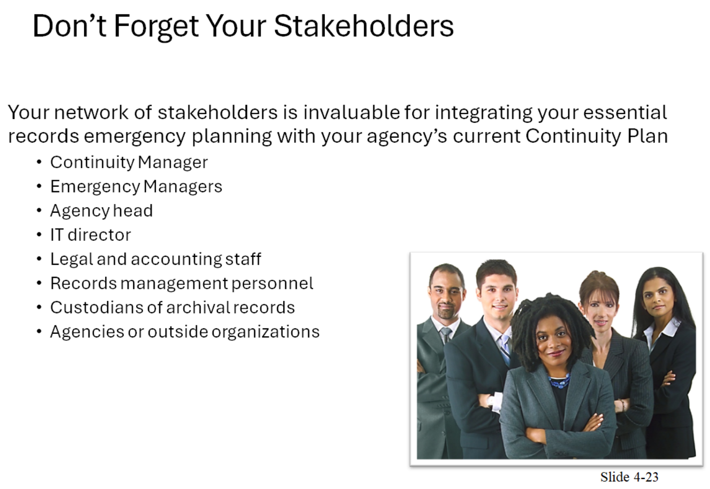
* Not every distinct essential record needs to be listed. Record series may suffice (e.g., death certificates, obviously, may be listed once), if at the same location and on the same medium or media.

The Essential Records Template is a suggested method for including essential records information in your agency's Continuity Plan. Use this template if your agency does not already have a template in place.

Refer to **Handout 4.4—Essential Records Template**, for a copy of the template.

Don’t Forget Your Stakeholders

Slide 4-23



Don’t Forget Your Stakeholders

Your network of stakeholders is invaluable for integrating your essential records emergency planning with your agency’s current Continuity Plan

- Continuity Manager
- Emergency Managers
- Agency head
- IT director
- Legal and accounting staff
- Records management personnel
- Custodians of archival records
- Agencies or outside organizations

Slide 4-23

At this point, your primary interest is to ensure that the essential records emergency planning you’ve completed and documented in your template is presented in a way that can be integrated with your agency’s current Continuity Plan and other emergency plans, so that essential records procedures are clear to all those preparing for and responding to emergencies.

Again, your network of stakeholders will be invaluable. The Continuity Manager and Emergency Manager in your agency should be consulted, so that they see how to integrate your work with the current emergency plan and training. The agency head (or designate) and IT Director should be briefed fully on aspects of your plan that will require resources—especially the recommendations for protecting records.

As noted during Session 1, your agency’s “stakeholders” include both the agencies and people you serve AND the agencies and people on whom you depend to provide that service, including:

- The Continuity Manager for your agency, who should be involved from the beginning so that you can ensure that essential records are fully addressed in the Continuity Plan
- Emergency Managers for your agency, as well as those in federal, state, and local government agencies, who should be consulted so that they can integrate your work with existing emergency plans and include essential records considerations in training courses
- First responders, who might be called in the event of an emergency, including police and fire fighters

- Agency head (or designate), who should be briefed fully on aspects of your plan that will require resources—especially those recommended for protecting records
- IT Director, who will also need to understand special considerations for providing access to essential records, beyond routine backup procedures
- Legal and accounting staff, who will ensure that all obligations are addressed in the plan
- Records management personnel who understand all of the records systems in the agency, understand who creates them, and knows how long they must be retained
- Custodians of the agency's archival records—i.e., those records that are worthy of permanent retention—who will be able to identify the records that have an overriding historical or cultural significance to the agency or the community
- Agencies or outside organizations that come to you often for information or services, and who can help you identify which records are essential to their operations and cannot be found elsewhere

If your agency depends on records in other agencies to support your ongoing operations, you'll want to ensure that that agency's records remain available during an emergency, or to make provisions to obtain critical information elsewhere.

Finally, one of the most important groups of stakeholders is the public. Residents of your state or locality depend on government to maintain and make available critical information that they will need to sustain their families and businesses after an emergency.

Course Review

Slide 4-24

Course Review

You now know how to:

- Identify records that need to be designated as essential
- Identify and evaluate risks to essential records
- Protect essential records
- Ensure continued access to essential records during and after an emergency
- Incorporate essential records into a Continuity Plan by using the Essential Records Template

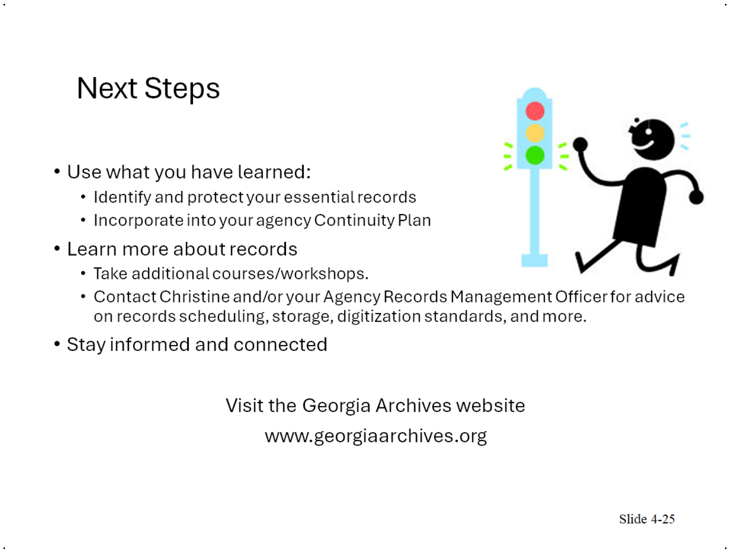
Slide 4-24

In the *Essential Records Course*, you learned:

- How to identify records that need to be designated as essential
- How to identify and evaluate risks to essential records
- How to protect essential records
- How to ensure continued access to essential records during and after an emergency
- How to incorporate essential records into a Continuity Plan by using the Essential Records Template

Next Steps

Slide 4-25



Next Steps

- Use what you have learned:
  - Identify and protect your essential records
  - Incorporate into your agency Continuity Plan
- Learn more about records
  - Take additional courses/workshops.
  - Contact Christine and/or your Agency Records Management Officer for advice on records scheduling, storage, digitization standards, and more.
- Stay informed and connected

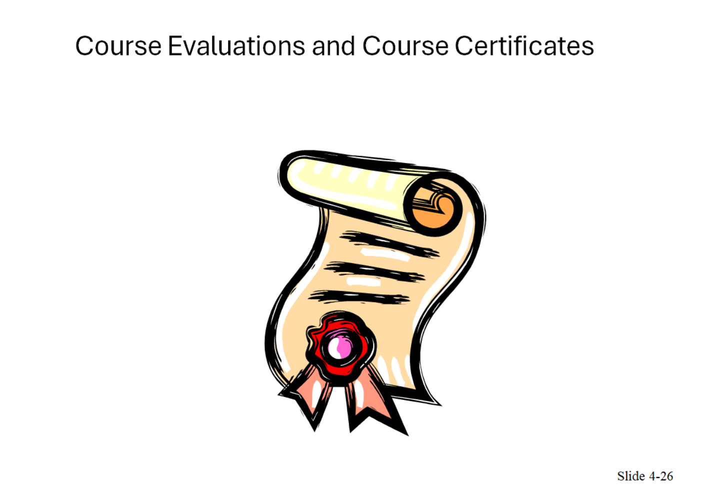
Visit the Georgia Archives website

www.georgiaarchives.org

Slide 4-25

Course Evaluations and Course Certificates

Slide 4-26



Course Evaluations and Course Certificates

Slide 4-26

Slide 4-27

Contacts

Christine Garrett
Manager of Records Management
Christine.Garrett@usg.edu

James Irby
Digital Preservation Technician
Sidney.Irby@usg.edu

Rebecca Wood
Records Manager
Rebecca.Wood@usg.edu

Sigourney Stanford
Conservator
Sigourney.Stanford@usg.edu

Christopher M. Davidson, J.D.
Assistant Vice Chancellor, State Archivist
Christopher.Davidson@usg.edu

Board of Regents of the University System of Georgia
IPER
Intergovernmental Preparedness for Essential Records
CoSA
Council of State Archivists
National Archives and Records Administration
FEMA

THANK YOU!