

Introduction to Incident Management & Response

Student Guide



Introduction to Incident Management & Response

Welcome & Introductions

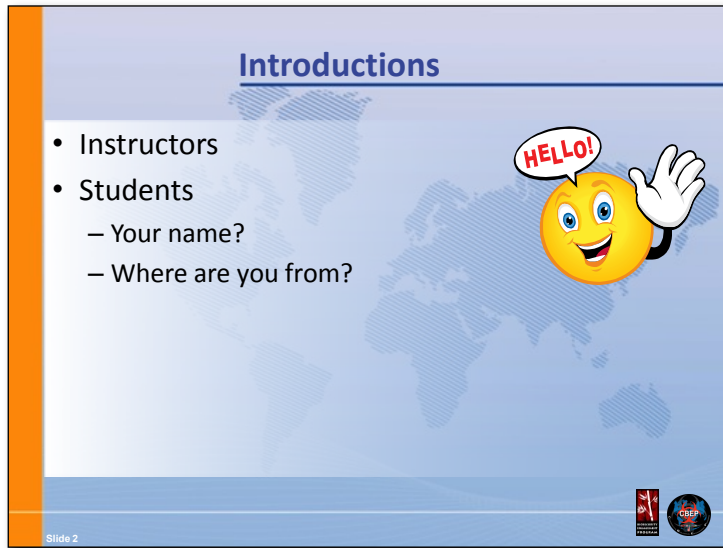
Welcome to Introduction to Incident Management & Response



Introduction to Incident Management & Response

Welcome & Introductions

Welcome to Introduction to Incident Management & Response



Action Plan

By the end of this lesson, I would like to:

KNOW		FEEL		BE ABLE TO DO	
------	--	------	--	---------------	--

Your learning doesn't stop with this lesson. Use this space to think about what else you need to do or learn to put the information from this lesson into practice.

What more do I need to know or do?	How will I acquire the knowledge or skills?	How will I know that I've succeeded?	How will I use this new learning in my job?

Use space on back, if needed





Introduction to Incident Management & Response

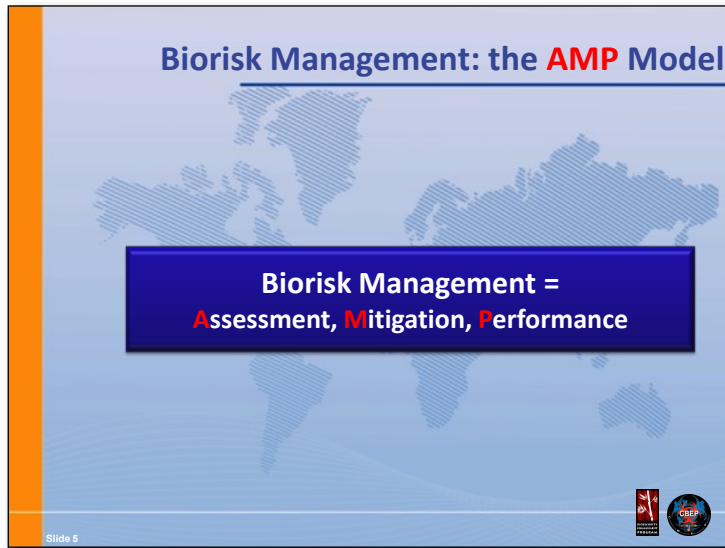
Welcome & Introductions

Course Objectives

- Understand the components and structure of an incident response system, including the roles and responsibilities of personnel involved in planning and notification of an incident.
- To know how to determine the effectiveness of an incident response system, why it is important, and how drills and exercises can be used to test the function and effectiveness of the system.
- Feel part of a team that can provide expertise and consultation on an incident response system as well as identify stakeholders to contribute to an incident response system.
- Determine how to implement an incident response system, including planning an preparation.




Slide 4





Record refresher notes on the AMP model and biorisk management.

Key Components of Biorisk Management

 **Biorisk Assessment**


- Process of identifying the hazards and evaluating the risks associated with biological agents and toxins, taking into account the adequacy of any existing controls, and deciding whether or not the risks are acceptable





Slide 6

Define Biorisk Assessment:

Key Components of Biorisk Management

 **Biorisk Mitigation**


- Actions and control measures that are put into place to reduce or eliminate the risks associated with biological agents and toxins





Slide 7

Define Biorisk Mitigation:

Key Components of Biorisk Management

 **Performance**

– The implementation of the entire biorisk management system, including evaluating and ensuring that the system is working the way it was designed. Another aspect of performance is the process of continually improving the system.



Slide 8

Define Performance:



Incident

Group Exercise:

In your groups, spend **5 minutes** to develop a **definition for an Incident**?

- To help with this task, list all possible examples of an **Incident** on sticky-notes and place them on your flip chart.

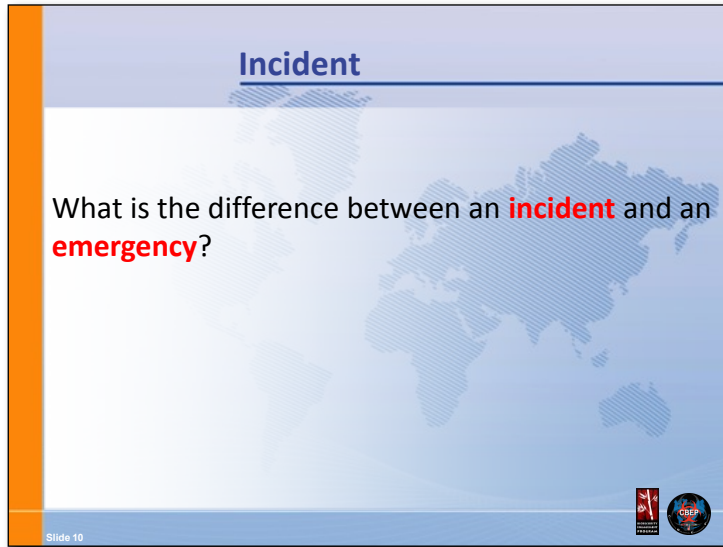
Once you are done, **write your definition at the top of the flip chart**, and be prepared to discuss with the rest of the class.



Slide 9

Define an incident:

What are some examples?





What is the difference between an incident and an emergency?

Notes:

Incident versus Emergency

An **incident** is an event that is likely to have adverse consequences.

An **emergency** is an **incident** that requires an immediate response.





Slide 11

Incident versus Emergency

Group Exercise - Continued:

Take **5 minutes** to look at your examples of **incidents** and categorize them as either an **incident** or an **emergency** especially in terms of biorisk.

Can you see the difference?



What is the difference between an incident and an emergency?

Notes:

Incidents

Some Things to Consider

1.

Some types of **incidents** can have adverse consequences that are relatively minor.

2.

However, **small incidents** can lead to **large** ones down the road, especially if they are frequent and **breed personnel complacency**.


1.

Society, the government and upper management often decide **what constitutes a large or small incident**. It is then up to management to **determine to what extent resources should be allocated** toward an **incident response management system**.

2.

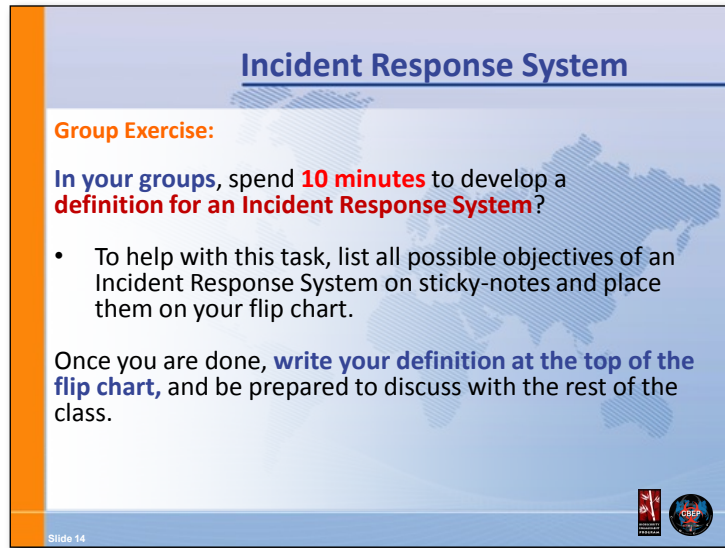
Because an **emergency** is simply a particular type of **incident**, an **Emergency Response System** will often form part of a **larger Incident Response System**.

Slide 13



Introduction to Incident Management & Response

What is an Incident Response System?



Incident Response System

Group Exercise:

In your groups, spend **10 minutes** to develop a **definition for an Incident Response System**?

- To help with this task, list all possible objectives of an Incident Response System on sticky-notes and place them on your flip chart.

Once you are done, **write your definition at the top of the flip chart**, and be prepared to discuss with the rest of the class.

Slide 14

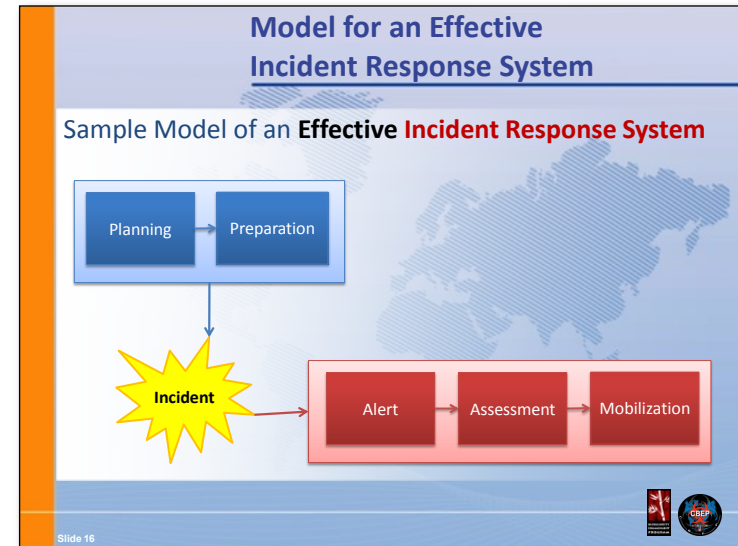
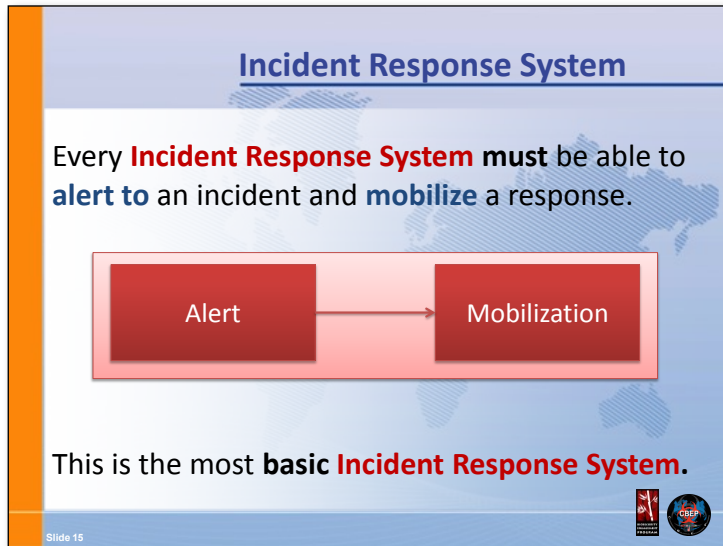
What is an Incident Response System?

Definition:

Objectives:

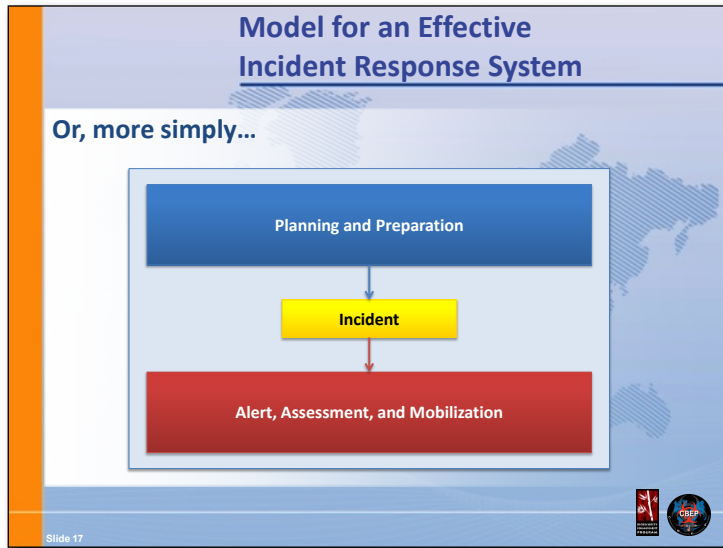
Introduction to Incident Management & Response

What is an Incident Response System?



Introduction to Incident Management & Response

What is an Incident Response System?



Incident Response System

The most **effective incident response systems** can **plan** and **prepare** for potential incidents, **alert** and **assess** actual incidents, and quickly **mount an effective response** if an incident occurs.

The slide is labeled 'Slide 18' in the bottom left corner and features a small logo in the bottom right corner.

Introduction to Incident Management & Response

What is an Incident Response System?

Examples:



Why are Planning and Preparation so important?

Planning and Preparation

Without proper **planning and preparation**, an **incident response system** would be unable to **alert** to an **incident** in a timely fashion, properly **assess** the **incident**, or **mobilize** effectively in response.


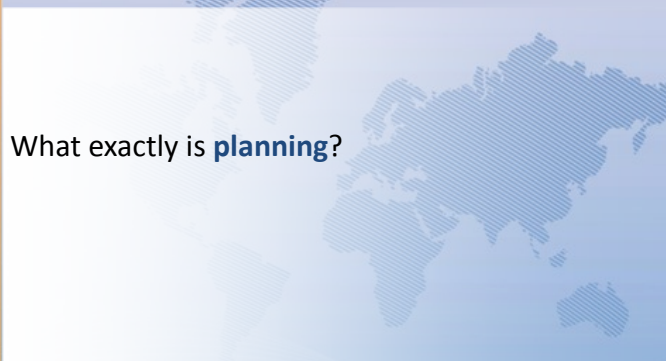
Why?

Hint: Think of an incident where there had not been any prior thought on how to respond. What was the outcome?

Slide 21

Planning

What exactly is **planning**?



Slide 22

Planning

Planning is the development of mechanisms or procedures, in advance, to achieve a particular goal.



Slide 23

Planning

In the case of **incident response**, **planning** is the process whereby a potential **incident** is **considered** and **evaluated**, and resources **are assigned**, in order to **generate** a response that will appropriately **mitigate** any adverse effects.

Slide 24



Planning

Incident response planning is normally the responsibility of an institution's **management**.

Top level **decision-makers** must come together to determine the best approach for handling **incidents** in a particular institution.

Slide 25



Planning

Management has the **authority** to make **medium** and **long-term decisions** and allocate appropriate **resources** towards an **incident management system**.

Management, however, needs the expertise and advise of other **personnel** in the institution to adequately make **plans**.

Why?

Slide 26

What is the role of Management in Incident Management & Response?


Planning

Group Exercise:

In your groups, spend **10 minutes** to **identify all the personnel** in an institution who could contribute to management's decisions during the planning phase of an incident response management system?

- Put each answer on a **sticky-note** and place them on your flip chart.
- Next to each personnel group, **list their role/contribution** to the planning process

Be prepared to discuss with the rest of the class.



Who can contribute to the Planning of an Incident Response System?

What is their contribution/role?

Planning

Often, **management** can develop high-level policy and delegate details to those **personnel** more familiar with daily operations and technical work.

Slide 29



Planning



Planning should result in a **document**, developed by **management** in cooperation with an institution's **personnel** (and others), that outlines, at a high-level, how the **incident management system** will operate.

Slide 30



Planning



The **document** should also contain further, specific details on **preparation**, **alert**, **assessment**, and **response** to an incident.



Slide 31

Preparation



What exactly is **preparation**?



Slide 32

Preparation



Preparation derives directly from **planning**. It is the act of putting into effect an institution's **plans** prior to an **incident**, in order to be in a position to better handle that **incident** when it does occur.



Slide 33

Preparation

The **Preparation** process includes **training** of **personnel**, acquisition of **equipment**, storing of **supplies**, and **physical modifications** to equipment and **buildings** when possible, and desirable.



Slide 34

Introduction to Incident Management & Response


Planning & Preparation

Preparation

Question: What kind of **information** should be included in a **planning document** in order to properly guide the **preparation** process?

In your groups, please discuss for **5 minutes** and write your ideas on separate **sticky notes**.

The class will make a **collection of sticky notes** to review each group's responses. **Did everyone come up with similar types of information?**



Slide 35

What type of information would be useful to be included in a planning document to guide the preparation process?

Introduction to Incident Management & Response

Planning & Preparation

Preparation

Think about the different types of **personnel** who work in a typical **lab** or **institution**.

Question: How should each of these be involved in the **preparation** process?

Please **discuss** for **5 minutes** at your **tables** and be prepared to share with the class.

Slide 36

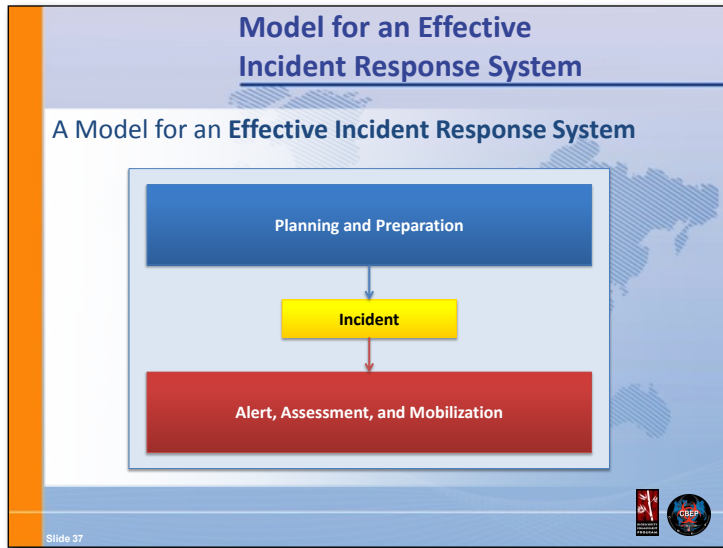
Who can contribute to the Preparation of an Incident Response System?

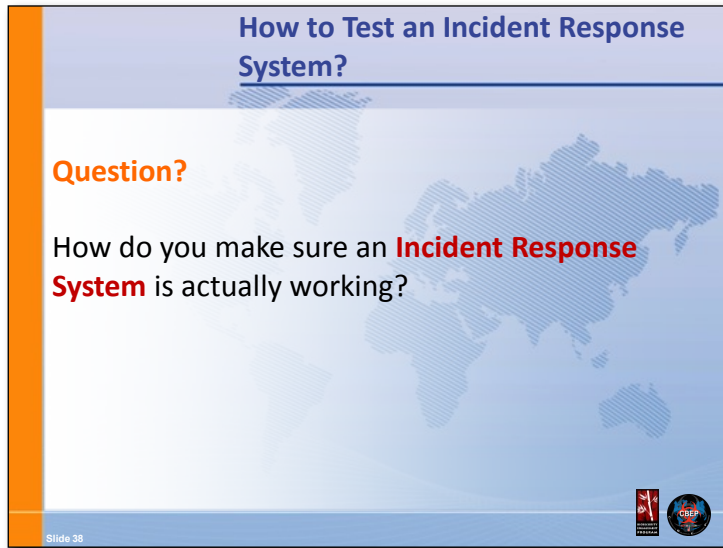
What is their contribution/role?

Introduction to Incident Management & Response

Planning & Preparation

Notes:





How can you test an Incident Response System?

How do drills help to validate an Incident Response System?

How to Test an Incident Response System? - Drills

Question?

How do you make sure an **Incident Response System** is actually working?

One way is by conducting **drills**.

Drills allow verification of whether a system is prepared to respond adequately to an **incident**, without actually putting a **facility** and its **personnel** at risk.

Slide 39


Introduction to Incident Management & Response


Drills


Notes:

Incident Response Systems



Thus, it is unreasonable to rely only on incidents to determine the effectiveness of an **Incident Response System**, instead Drills are used to simulate incidents.

Planning and Preparation 

Incident and Drills 

Alert, Assessment, and Mobilization 

Slide 40

Drills

Group Exercise:

Question: What different kinds of **drills** can an **institution** use to test their **incident response system**, especially in terms of incidents impacting biorisk?

Take 5 minutes to discuss the question and **make a table**, on your flip chart, **listing the advantages and disadvantages of each kind of drill**. Be prepared to share your discussion with the class.

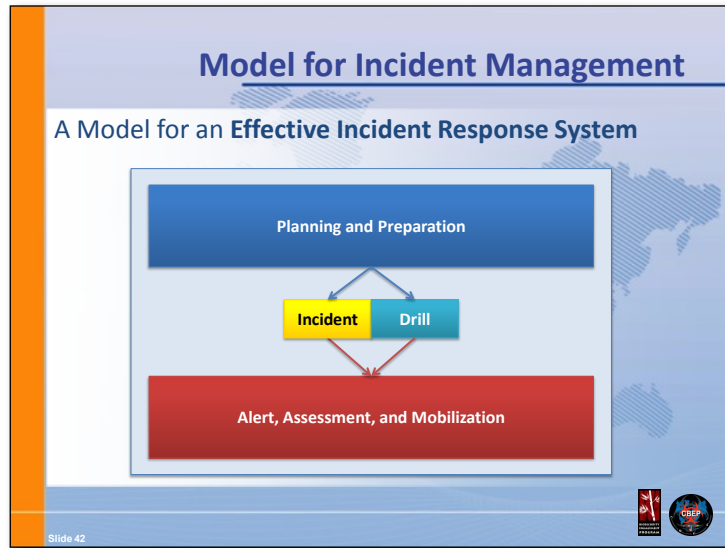
Slide 41

List some different types of drills

Advantages?

Disadvantages?

Notes:



Alert

Alerting is the process of identifying an **incident** as it is occurring, or after it has occurred, and using that information to **generate a response**.

Questions:
What are some ways one could **alert**?
Who would you **alert**?

Slide 43

What are some ways one could alert?

Who would you alert?

Notes:

Alert

An institution's **incident response plan**, as developed by **management**, should address **procedures** for **alerting** appropriate **personnel** in the event of an **incident**.



Slide 44

Introduction to Incident Management & Response

Alert, Assessment and Mobilization

Alert

Question: How would one determine whether **alerting** should occur during an **incident**, or after the **incident**?

Please consider this question for **5 minutes** and be prepared to discuss with the class.

Hint: What are the key factors about the incident that would make a difference about when to alert?

Slide 45



When does alerting happen during the incident?

When does alerting happen after the incident?

Assessment

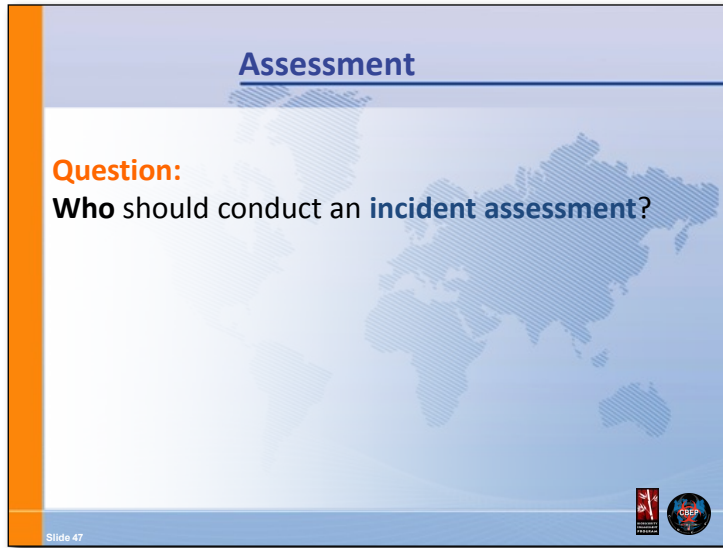
In part, the answer to the previous question is a matter of **assessment**.

Assessment is the evaluation of the type and severity of an **incident**, in order to determine an appropriate response.



Slide 46

How does Assessment play a role in an Incident Response System?




Who should conduct an Incident Assessment?

Assessment

Question: How do you assess an incident?

In your tables, please consider this question for **5 minutes**, and list all the criteria by which an incident can be assessed. Put each criteria on a sticky-note.

Slide 48



How would you assess an incident?

What factors would you consider?

What are the criteria you would use?



<hr/>	<hr/>
<hr/>	<hr/>
<hr/>	<hr/>
<hr/>	<hr/>
<hr/>	<hr/>

Notes:

Alerting and Assessment

Alerting and **assessment** provide information as to the existence and nature of a particular **incident**.

Some **incidents** are self-resolving, and by the time an **alert** is raised and the **incident** is **assessed**, a specific response may not be needed.




Slide 49

Mobilization

Mobilization is the activation of **personnel** and use of **equipment** to respond directly to an **incident** and hasten its **resolution**.

Question: What are some factors that determine the mobilization?



Slide 50

What is Mobilization?

What are some factors that determine the mobilization?

Introduction to Incident Management & Response

Alert, Assessment and Mobilization

When and who determines when an incident is resolved?

Mobilization

Questions:
When an incident is considered to be resolved?
Who determines that an incident is resolved?

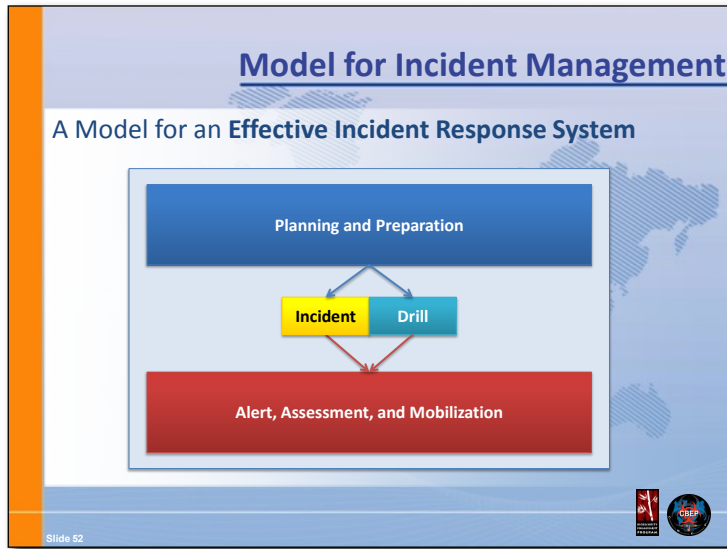
Please consider this question for **5 minutes** and be prepared to discuss with the class.

Slide 51

Introduction to Incident Management & Response

Feedback

Notes:



Feedback

Feedback is the use of **information** gathered from **drills** or **incidents** to inform and improve an **Incident Response System**.

Specifically, **feedback** informs the **planning and preparation** process, providing information to **management** and other **personnel** on what procedures were and were not effective in mitigating the adverse consequences of incidents (or drills).




Slide 53

Feedback

Feedback could be considered a fourth phase of an **Incident Response System**.

Planning and Preparation 

Incidents and Drills 

Alert, Assessment, and Mobilization 

Feedback 

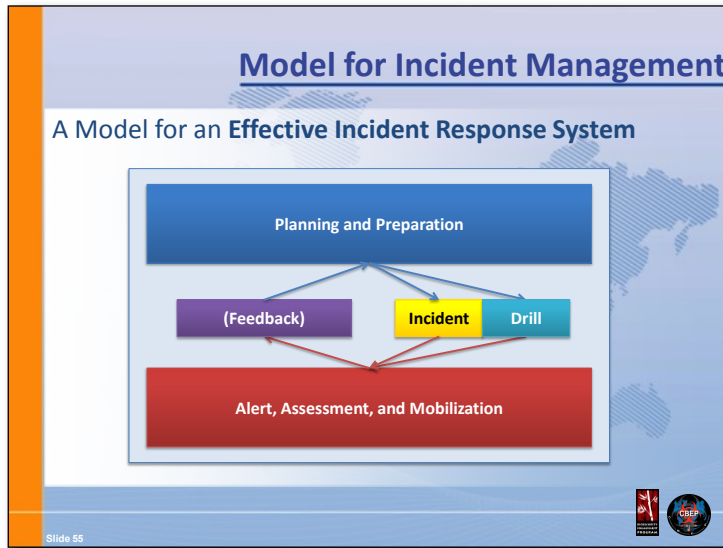


Slide 54

Introduction to Incident Management & Response

Feedback

Notes:



Introduction to Incident Management & Response

Feedback

Feedback

Question: What types of information are necessary to provide feedback that addresses the strengths and weaknesses – success and failures – of the current incident response system?

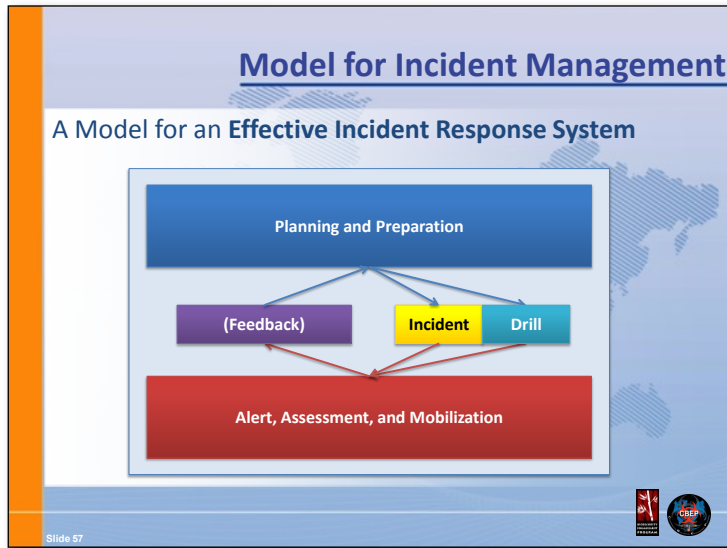
Please spend **10 minutes** discussing the question in **your table**, and be prepared to share your thoughts with the class.

Hint: List 7 to 10 questions you would ask after a drill or incident to help gather this information.

Slide 56

What types of feedback helps strengthen the Incident Response System?

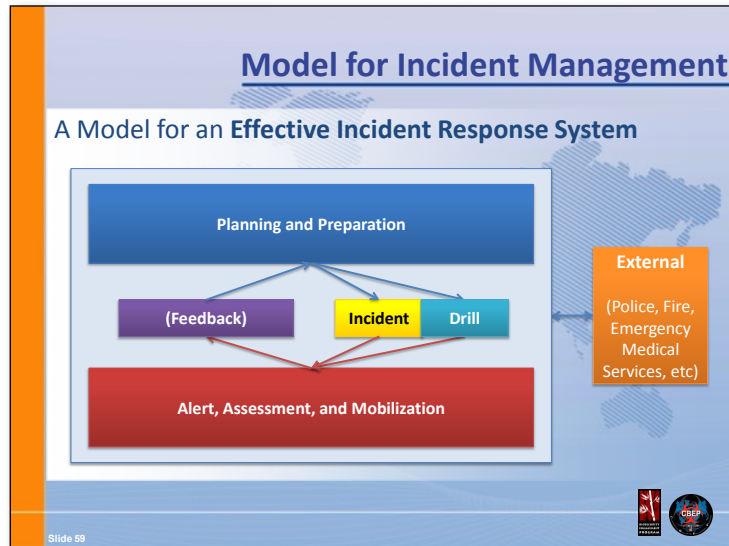
What are some questions you would ask after a drill or incident?



Outside Responders

As part of both **planning and preparation** as well as **alerting, assessment, and response**, an **incident response system** must interact with the **outside world** in order to properly manage serious incidents.

The slide is labeled 'Slide 58' in the bottom left corner and includes a small logo in the bottom right corner.



Outside Responders

It is often not economical for an **institution** to develop the capacity to respond to large, infrequent **incidents** and **emergencies** completely on its own.

Also, depending on the laws of the jurisdiction that an institution is located in, there might be certain kinds of incidents that the institution cannot respond to.

Thus, coordination with **police, fire brigades, and emergency medical services** are crucial for effective **incident response**.

The slide is labeled 'Slide 60' in the bottom left corner and includes a small logo in the bottom right corner.

Introduction to Incident Management & Response


Outside Coordination

Outside Coordination

Question: How would **outsiders** such as the **fire brigade** interact with an institution during each of these incident response system phases?

- **Planning and Preparation**
- **Alert & Assessment**
- **Mobilization**
- **Feedback**

In your tables, please spend **10 minutes** discussing these questions and be prepared to share your table's thoughts with the class.



Slide 61

How do outsiders interact with an institution during each of the Incident Response System Phases?

Planning and Preparation?

Alert & Assessment?

Mobilization?

Feedback?

Review

Review Question: What are the four phases of an effective **Incident Response System**?




Slide 62

Review

Review Question:

What is the difference between an **Emergency Response System** and an **Incident Response System**?



Slide 63

Introduction to Incident Management & Response

Review

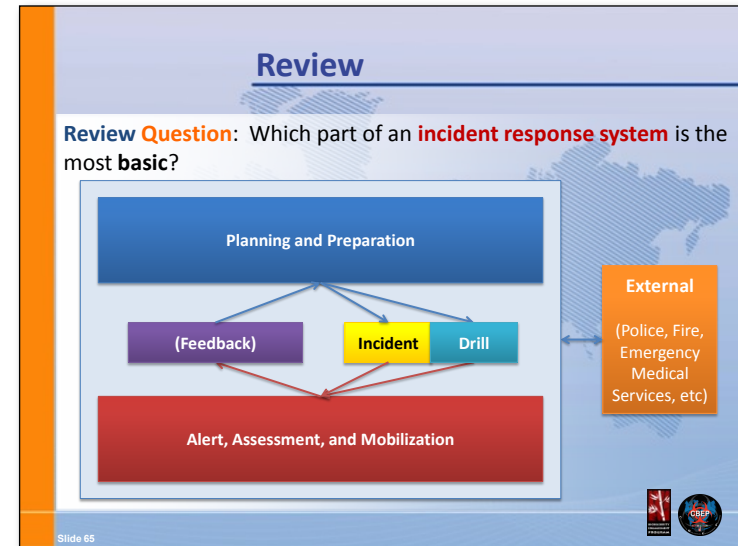
Review

Review Question: Do you agree with this table? Why or why not?

Responsibilities in an Incident Response System

	Management	Other Personnel
Planning and Preparation	Yes	No
Alerting, Assessment, and Response	Yes	Yes
Feedback	Yes	Yes

Slide 64



Introduction to Incident Management & Response

Review


Notes:

Review

Review Question:

Why is **outside coordination** so important for an **incident response system**?

Slide 66



Introduction to Incident Management & Response

Review

Review of Introduction to Incident Management & Response

Review

For **10 minutes**, let's discuss what we have learned about **incident response systems**.

What did we learn?	What does it mean?	Where do we go from here?
--------------------	--------------------	---------------------------

Slide 67


Small logos for NIST and CBEP are visible in the bottom right corner of the slide.

Introduction to Incident Management & Response

Review

Review - Course Objectives

- Understand the components and structure of an incident response system, including the roles and responsibilities of personnel involved in planning and notification of an incident.
- To know how to determine the effectiveness of an incident response system, why it is important, and how drills and exercises can be used to test the function and effectiveness of the system.
- Feel part of a team that can provide expertise and consultation on an incident response system as well as identify stakeholders to contribute to an incident response system.
- Determine how to implement an incident response system, including planning and preparation.



Slide 68
