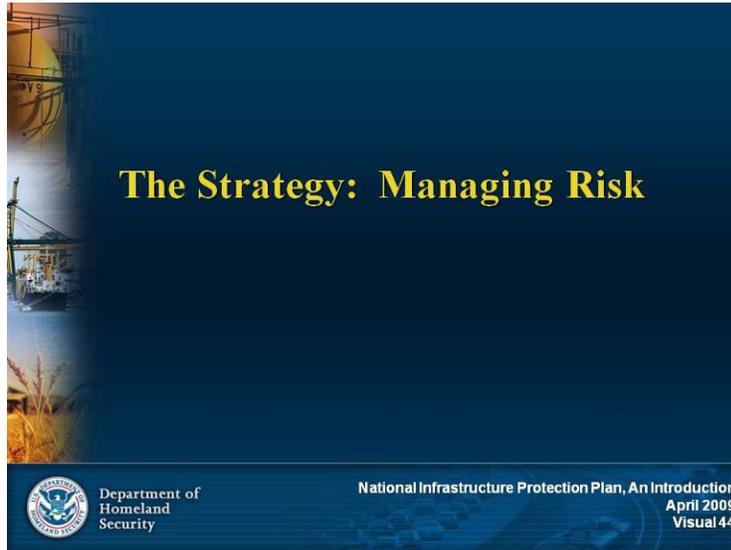


Visual 44



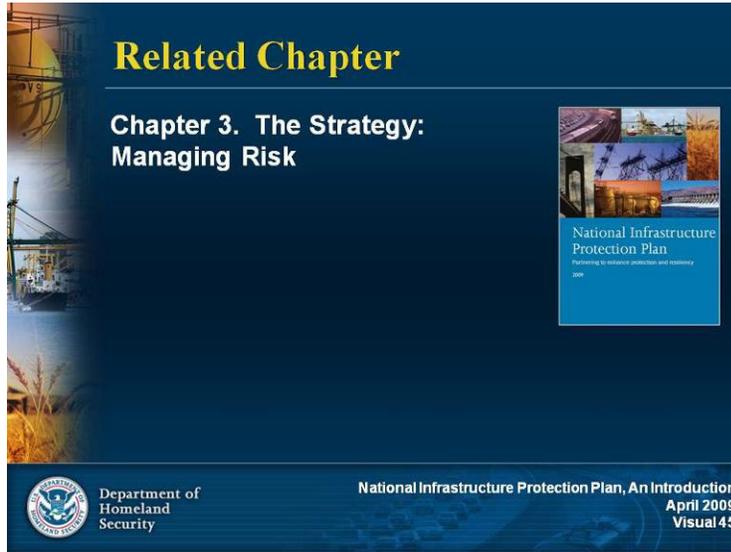
Visual Description: The Strategy: Managing Risk

Key Points

The cornerstone of the NIPP is its risk management framework. This framework establishes the processes for combining consequence, vulnerability, and threat information to produce comprehensive and objective assessments of national or sector risk. The risk management framework is structured to promote continuous improvement to enhance CIKR protection.”

This section of the course reviews the NIPP’s risk management framework.

Visual 45



Visual Description: Related Chapter

Key Points

This portion of the course summarizes the information presented in Chapter 3 of the NIPP, titled “The Strategy: Managing Risk.”

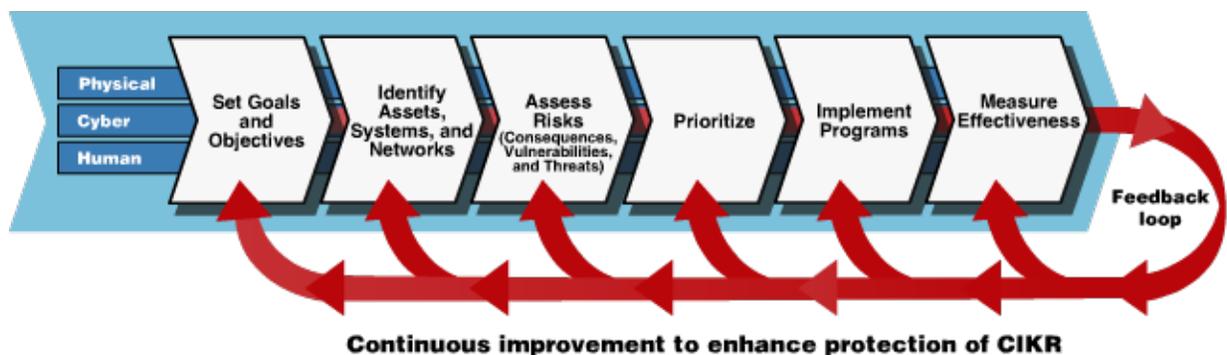
Visual 46



Visual Description: Risk Management Framework

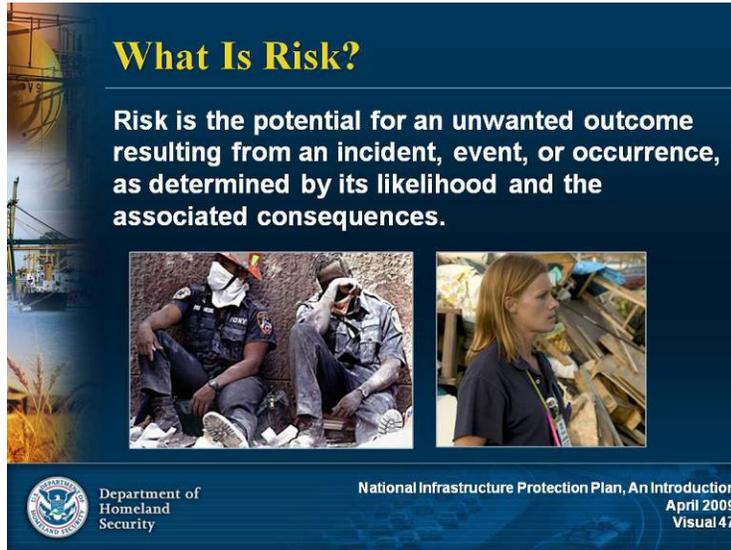
Key Points

The NIPP risk management framework establishes a process for identifying risks and prioritizing protection and resiliency initiatives and investments within and across sectors. The objective is to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risk.



Caption: Graphic showing the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.

Visual 47



What Is Risk?

Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Department of Homeland Security

National Infrastructure Protection Plan, An Introduction
April 2009
Visual 47

Visual Description: What Is Risk?

Key Points

Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Risk is influenced by the nature and magnitude of a threat, the vulnerabilities to that threat, and the consequences that could result.

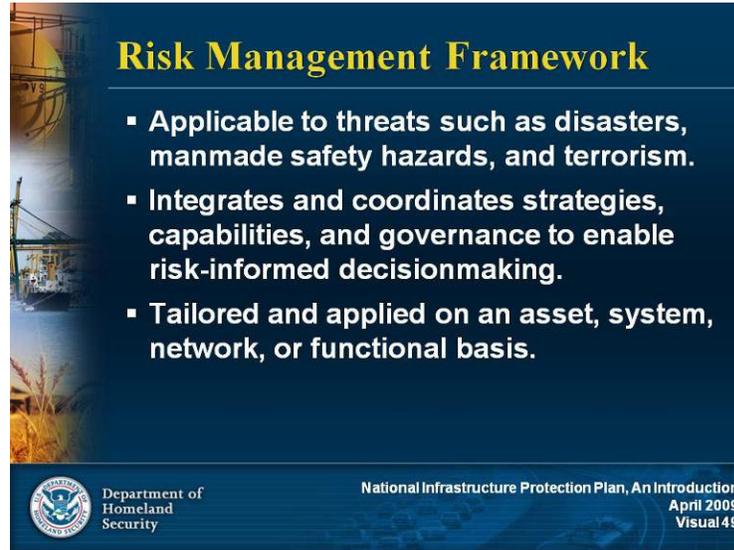
Visual 48

**Visual Description:** Risk Management Framework**Key Points**

The NIPP risk management framework is structured to promote continuous improvement to enhance CIKR protection by focusing activities on efforts to:

- Set goals and objectives.
- Identify assets, systems, and networks.
- Assess risks (consequences, vulnerabilities, and threats).
- Establish priorities based on risk assessment.
- Implement protective programs and resiliency strategies
- Measuring effectiveness.

Visual 49



Visual Description: Risk Management Framework

Key Points

The risk management framework:

- Is applicable to threats such as disasters, manmade safety hazards, and terrorism.
- Integrates and coordinates strategies, capabilities, and governance to enable risk-informed decisionmaking.
- Is tailored and applied on an asset, system, network, or functional basis, depending on the fundamental characteristics of the individual CIKR sectors.

Sectors primarily dependent on fixed assets and physical facilities may use a bottom-up, asset-by-asset approach. A top-down, business or mission continuity approach may be more effective for sectors with accessible and distributed systems.

Visual 50

Risk Management Responsibilities: DHS

Department of Homeland Security (DHS):

- Supports risk management efforts by providing guidance and analytical support to SSAs and other partners.
- Conducts cross-sector risk analysis in collaboration with other CIKR partners.
- Works with CIKR partners to identify and share threat information, lessons learned, and best practices.

Department of Homeland Security

National Infrastructure Protection Plan, An Introduction
April 2009
Visual 50

Visual Description: Risk Management Responsibilities: DHS

Key Points

DHS is responsible for:

- Supporting risk management efforts by providing guidance and analytical support to SSAs and other partners.
- Using the best available information to conduct cross-sector risk analysis and risk management activities in collaboration with other CIKR partners.
- Working with CIKR partners to identify and share threat information, lessons learned, and best practices for all aspects of the risk management process.

Visual 51

Risk Management Responsibilities: SSAs

Sector-Specific Agencies (SSAs):

- Develop and implement Sector-Specific Plans with their respective sector partners.
- Foster communication with sector partners.
- Coordinate sector-specific risk management programs.
- Prioritize sector risks and needs, in conjunction with sector partners.

Department of Homeland Security

National Infrastructure Protection Plan, An Introduction
April 2009
Visual 51

Visual Description: Risk Management Responsibilities: SSAs

Key Points

SSAs are responsible for:

- Developing and implementing Sector-Specific Plans (SSPs) with their respective sector partners.
- Fostering communication with sector partners.
- Coordinating sector-specific risk management programs.
- Prioritizing sector risks and needs, in conjunction with sector partners.

Visual 52

Physical, Cyber, and Human Elements

The risk management framework encompasses:

- **Physical Elements** – tangible property
- **Cyber Elements** – electronic information and communications systems, and the information contained therein
- **Human Elements** – critical knowledge of functions or people uniquely susceptible to attack

Physical
Cyber
Human

Department of Homeland Security
National Infrastructure Protection Plan, An Introduction
April 2009
Visual 52

Visual Description: Physical, Cyber, and Human Elements

Key Points

The risk management framework is comprehensive and takes into account the assets, systems, and networks that include one or more of the following elements:

- **Physical** – tangible property
- **Cyber** – electronic information and communications systems, and the information contained therein
- **Human** – critical knowledge of functions or people uniquely susceptible to attack

Visual 53

Cyber Elements

The NIPP addresses reducing cyber risk and enhancing cybersecurity as a:

- Cross-sector cyber element that involves DHS, SSAs, and private-sector owners and operators; and
- Major component of the Information Technology Sector's responsibility in partnership with the Communications Sector.

Department of Homeland Security
National Infrastructure Protection Plan, An Introduction
April 2009
Visual 53

Visual Description: Cyber Elements**Key Points**

- The U.S. economy and national security are highly dependent upon the global cyber infrastructure. Cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent global network of CIKR.
- A spectrum of malicious actors could conduct attacks against the cyber infrastructure using cyber attack tools. Because of the interconnected nature of the cyber infrastructure, these attacks could spread quickly and have a debilitating impact.
- The use of innovative technology and interconnected networks in operations improves productivity and efficiency, but also increases the Nation's risk to cyber threats if cybersecurity is not addressed and integrated appropriately.
- The interconnected and interdependent nature of the Nation's CIKR makes it problematic to address the protection of physical and cyber assets independently.
- The NIPP addresses reducing cyber risk and enhancing cybersecurity in two ways: (1) as a cross-sector cyber element that involves DHS, SSAs, and private sector owners and operators; and (2) as a major component of the Information Technology (IT) Sector's responsibility in partnership with the Communications Sector.

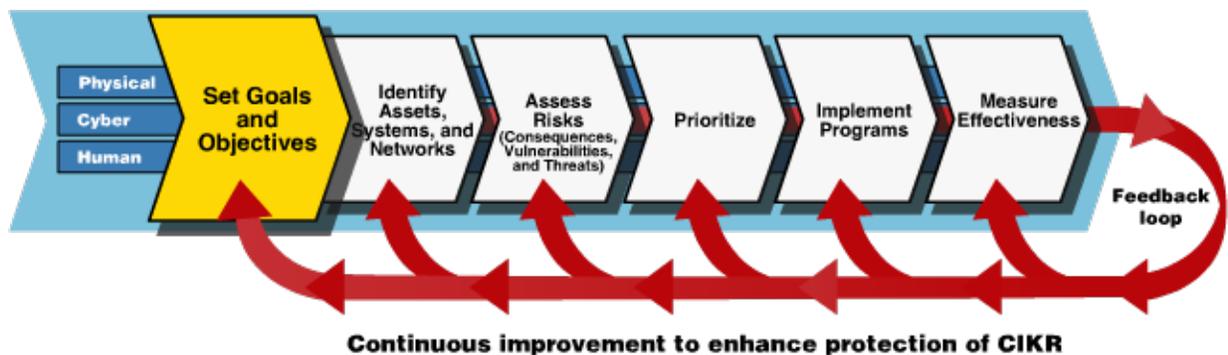
Visual 54



Visual Description: Set Goals and Objectives

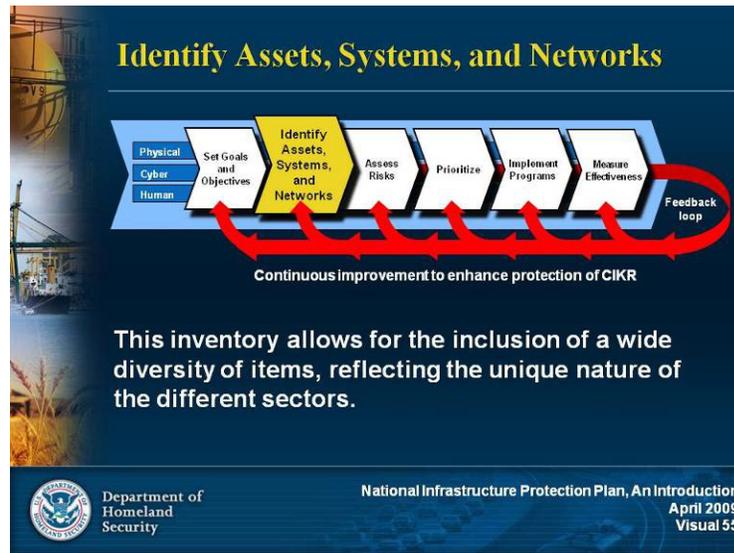
Key Points

The process begins by setting goals and objectives. CIKR partners work together to define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective risk management posture.



Caption: Graphic showing the role setting goals and objectives plays in the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.

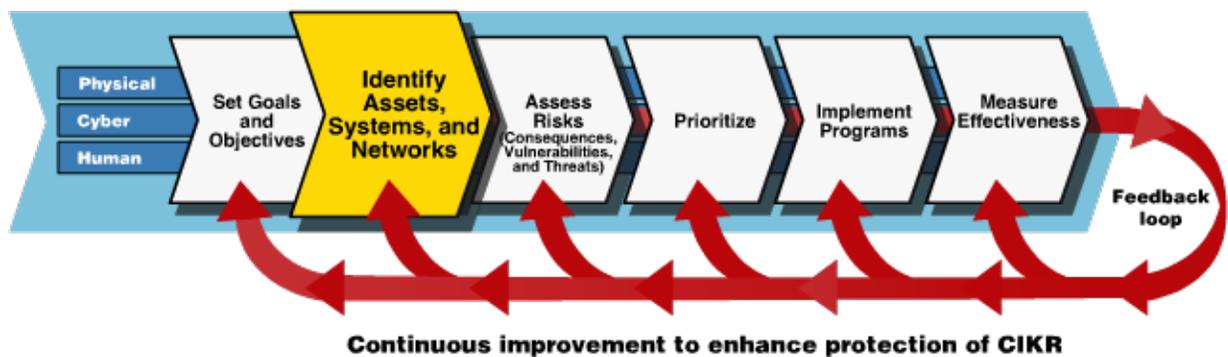
Visual 55



Visual Description: Identify Assets, Systems, and Networks

Key Points

After setting goals, the next activity is to develop and maintain an inventory of the assets, systems, and networks—including those located outside the United States – that comprise the Nation’s CIKR and their functions. The inventory allows for the inclusion of a wide diversity of items, reflecting the unique nature of the different sectors.



Caption: Graphic showing the role identifying assets, systems, and networks plays in the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.

Visual 56



Visual Description: Assess Risks

Key Points

Risk is assessed as a function of consequence, vulnerability, and threat. Consideration is given to the potential direct and indirect consequences of a terrorist attack or other hazards, known vulnerabilities to those threats or hazards, and the nature and magnitude of the threat.

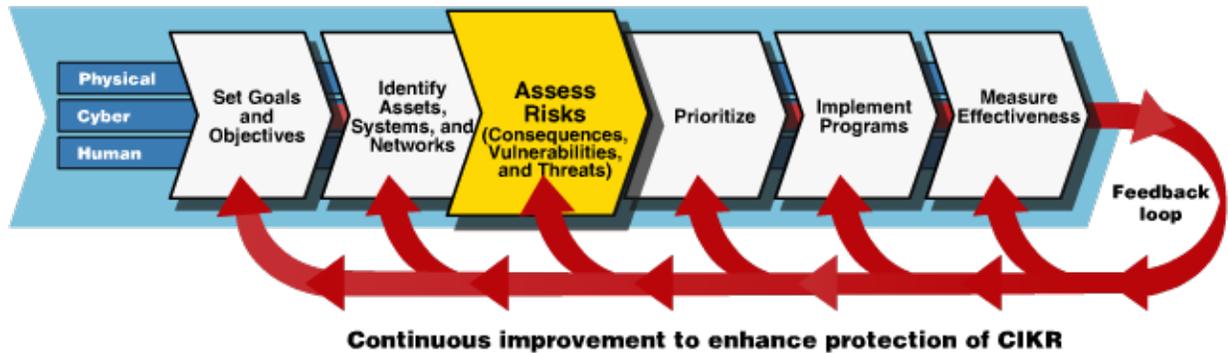
- Calculating Risk.** Risk assessments are conducted on an asset, system, or network basis. For some sectors, an asset-based approach is most effective; for others, particularly those with virtual or information-based core processes, assessing system or network risk and resiliency is more appropriate.

Once the three components of risk—consequence, vulnerability, and threat—have been assessed for one or more given assets, systems, or networks they must be integrated into a defensible model to produce a risk estimate. DHS has identified a number of risk assessment characteristics and data requirements to produce results that enable cross-sector risk comparisons; these are termed core criteria. These features provide a guide for improving or modifying existing methodologies as well as developing new ones.

- Use of Existing Risk Assessment Tools.** Many owners and operators perform vulnerability and/or risk assessments on the assets, systems, and networks under their control. To take advantage of this existing body of work, DHS works with sectors to use the results from previously performed assessments wherever possible.

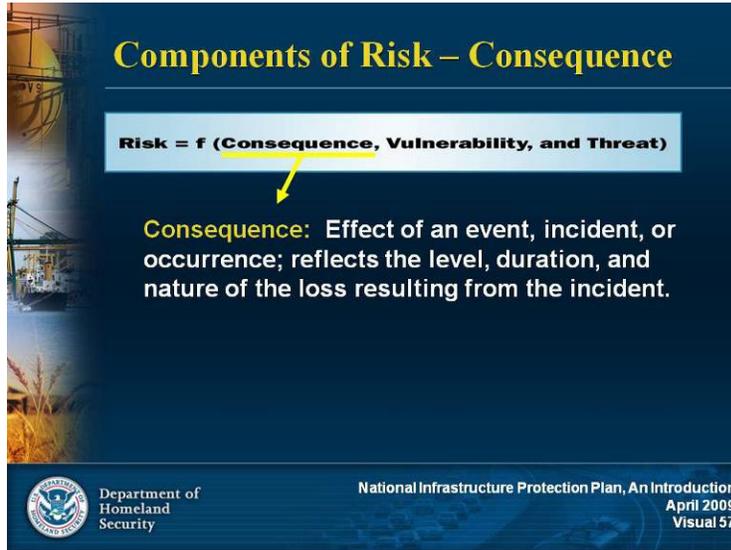
DHS and the SSAs work with partners to ensure that risk assessment tools and methodologies that are compatible with the NIPP core criteria are available. DHS will leverage and incorporate work already done, to the greatest extent possible, and will help tailor existing tools to meet the core criteria as required.

Note: A larger version of the illustration on the visual is provided on the following page.



Caption: Graphic showing the role assessing risks plays in the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.

Visual 57



Visual Description: Components of Risk—Consequence

Key Points

In the context of homeland security, CIKR partners assess risk as a function (f) of consequence, vulnerability, and threat.

Consequence is the effect of an event, incident, or occurrence; reflects the level, duration, and nature of the loss resulting from the incident.

For the purposes of the NIPP, consequences are divided into four main categories: public health and safety (i.e., loss of life and illness), economic (direct and indirect), psychological, and governance/mission impacts.

Visual 58

Components of Risk – Vulnerability

Risk = f (Consequence, Vulnerability, and Threat)

Vulnerability: A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

Department of Homeland Security
National Infrastructure Protection Plan, An Introduction
April 2009
Visual 58

Visual Description: Components of Risk—Vulnerability

Key Points

Vulnerability is a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

In calculating the risk of an intentional hazard, a common measure of vulnerability is the likelihood that an attack is successful, given that it is attempted.

Visual 59

Components of Risk – Threat

Risk = f (Consequence, Vulnerability, and Threat)

Threat: A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Department of Homeland Security
National Infrastructure Protection Plan, An Introduction
April 2009
Visual 59

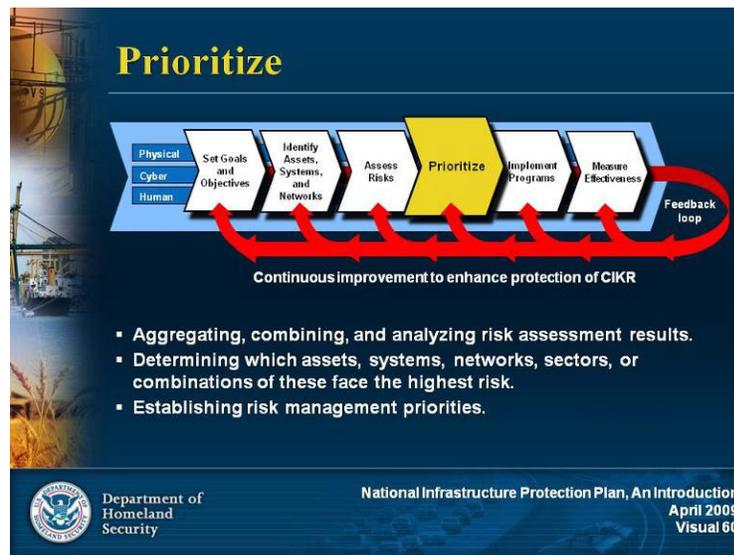
Visual Description: Components of Risk—Threat

Key Points

Threat is a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

For the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack being attempted by an adversary; for other hazards, threat is generally estimated as the likelihood that a hazard will manifest itself. In the case of terrorist attacks, the threat likelihood is estimated based on the intent and capability of the adversary.

Visual 60



Visual Description: Prioritize

Key Points

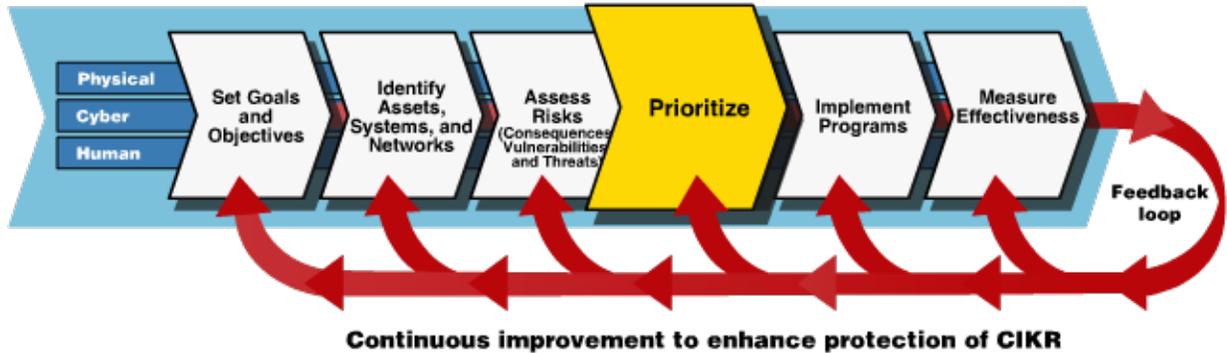
The prioritization process involves aggregating, combining, and analyzing risk assessment results to determine which assets, systems, networks, sectors, or combinations of these face the highest risk so that risk management priorities can be established. It also provides the basis for understanding potential risk-mitigation benefits that are used to inform planning and resource decisions.

- **The Prioritization Process.** The NIPP risk management framework provides the process for developing comparable estimates of the risk relevant to CIKR.

Comparing the risk faced by different entities helps identify where risk mitigation is most needed, and to subsequently determine and help justify the most cost-effective risk management options.

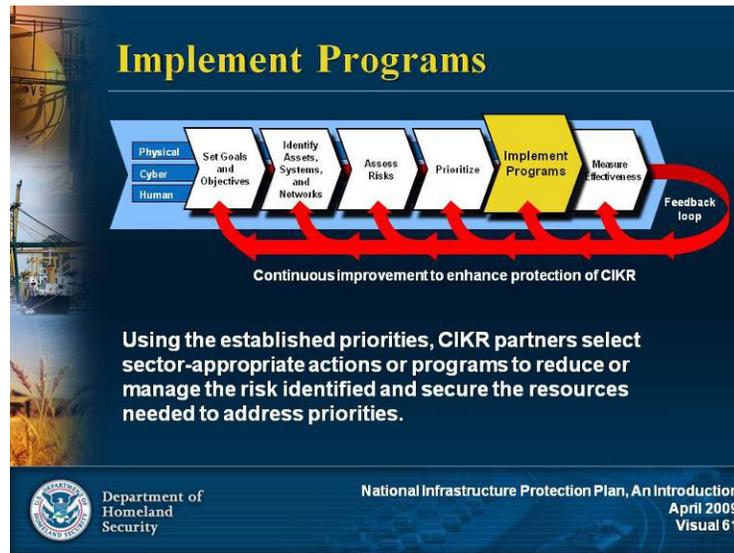
In addition, this prioritization process develops information that can be used during incident response to help inform decisionmakers regarding issues associated with CIKR restoration.

Note: A larger version of the illustration on the visual is provided on the following page.



Caption: Graphic showing the role establishing priorities plays in the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.

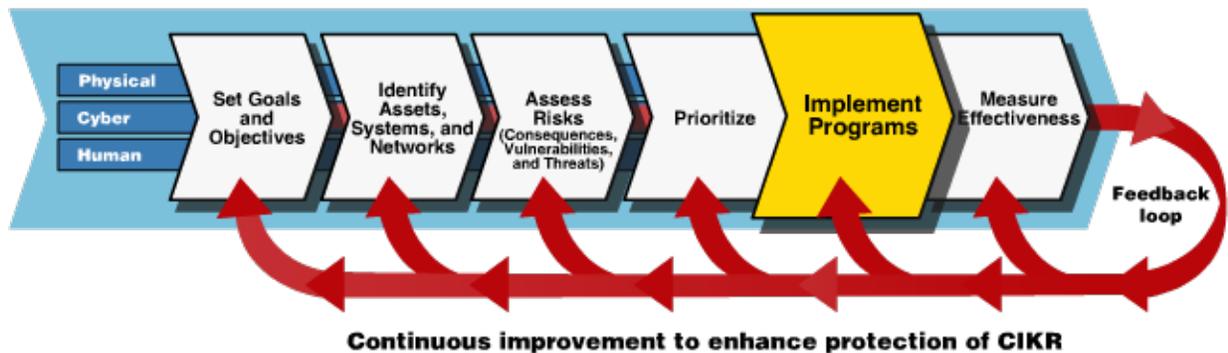
Visual 61



Visual Description: Implement Programs

Key Points

The risk assessment and prioritization processes help identify requirements for protective programs and resiliency strategies. Depending on the situation, the requirements may be filled by owners/operators, sector programs, State initiatives, or through cross-sector or national initiatives undertaken by DHS.



Caption: Graphic showing the role implementing protective programs and resiliency strategies plays in the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.

Visual 62

**Visual Description:** Risk Management Actions**Key Points**

Risk management actions involve measures designed to:

- Prevent, deter, and mitigate threats.
- Reduce vulnerability to an attack or other disaster.
- Minimizing consequences.
- Enable timely, efficient response and restoration.

Effective CIKR protective programs and resiliency strategies are:

- Comprehensive.
- Coordinated.
- Cost effective.
- Risk-informed.

Note: A larger version of the illustration on the visual is provided on the following page.



Caption: Graphic showing that the NIPP enhances protection of the Nation's CIKR by using risk management actions and programs and resiliency strategies, including cybersecurity, exercises, increasing awareness, personnel surety, physical measures, plans, reducing attractiveness, redundancy, reliability, resiliency, sharing information, and training.

Topic

The Strategy: Managing Risk

Risk management actions involve measures designed to prevent, deter, and mitigate the threat; reduce vulnerability to an attack or other disaster; minimize consequences; and enable timely, efficient response and restoration in a post-event situation—whether a terrorist attack, natural disaster, or other incident. Risk management actions include:

Action	Definition	Examples
Deter	Cause the potential attacker to perceive that the risk of failure is greater than that which they find acceptable.	<ul style="list-style-type: none"> ▪ Improved awareness and security (e.g., restricted access, vehicle checkpoints). ▪ Enhanced police and/or security officer presence.
Devalue	Reduce the attacker's incentive by reducing the target's value.	<ul style="list-style-type: none"> ▪ Developing redundancies. ▪ Maintaining backup systems or key personnel.
Detect	Identify potential attacks and validate and/or communicate the information, as appropriate.	<ul style="list-style-type: none"> ▪ Intelligence gathering. ▪ Analysis of surveillance activities. ▪ Trend analysis of law enforcement reporting. ▪ Intrusion-detection systems. ▪ Network monitoring systems. ▪ Operation alarms. ▪ Surveillance detection and reporting. ▪ Employee security awareness programs.
Defend	Protect assets by preventing or delaying the actual attack, or reducing an attack's effect on an asset, system, or network.	<ul style="list-style-type: none"> ▪ Perimeter hardening by enhancing buffer zones, fencing, and structural integrity. ▪ Cyber defense tools such as antivirus software.

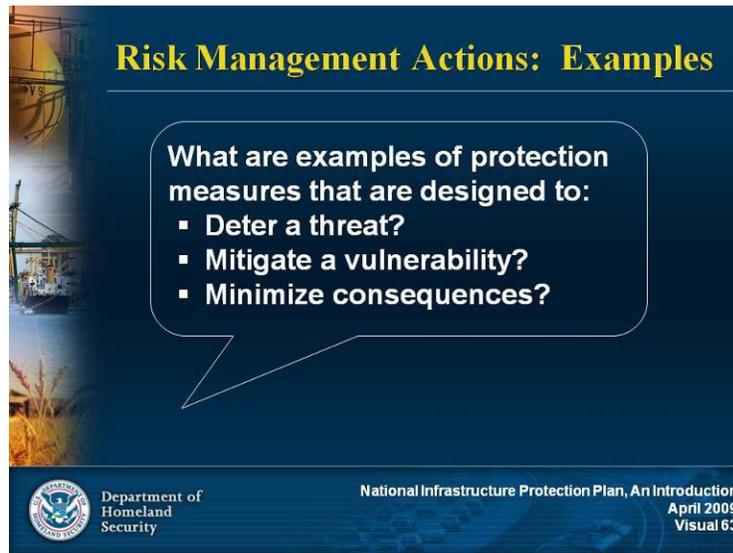
Risk management programs also may include actions that mitigate the consequences of an attack or incident. These actions are focused on the following aspects of preparedness:

Action	Definition	Examples
Mitigate	Lessen the potential impacts of an attack, natural disaster, or accident.	<ul style="list-style-type: none"> ▪ Introducing system redundancy and resiliency. ▪ Reducing asset dependency. ▪ Isolating downstream assets.
Respond	Enable rapid reaction and emergency response to an incident.	<ul style="list-style-type: none"> ▪ Conducting exercises. ▪ Having adequate crisis response plans, training, and equipment.
Recover	Allow businesses and government organizations to resume operations quickly and efficiently.	<ul style="list-style-type: none"> ▪ Using comprehensive mission and business continuity plans that have been developed through prior planning.

Topic

Activity

Visual 63



Visual Description: Risk Management Actions: Examples

Key Points

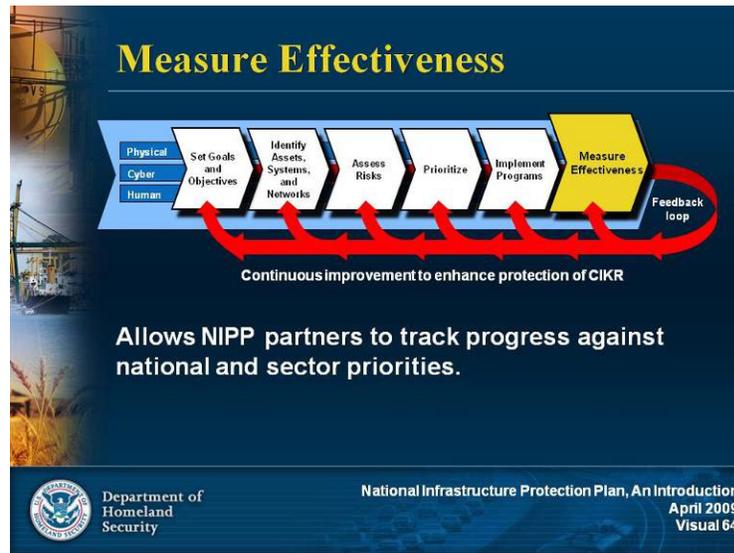
Provide some examples of protection measures that are designed to:

- Deter a threat.
- Mitigate a vulnerability.
- Minimize consequences.

Topic

The Strategy: Managing Risk

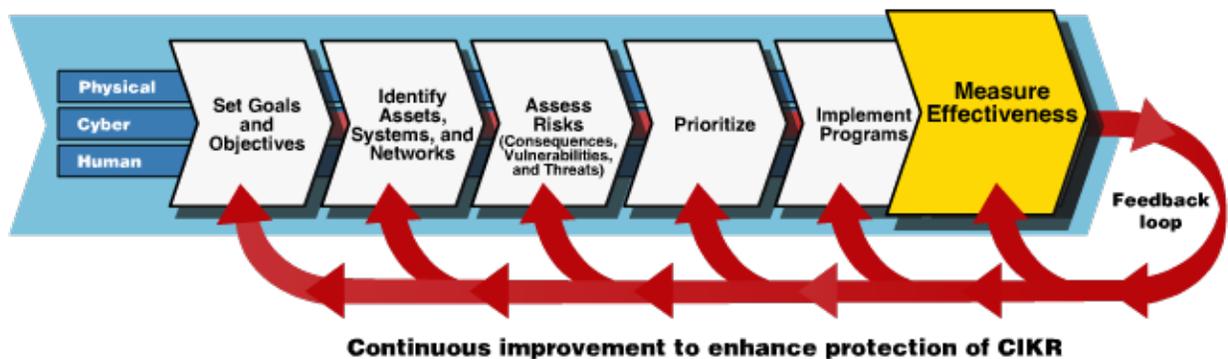
Visual 64



Visual Description: Measure Effectiveness

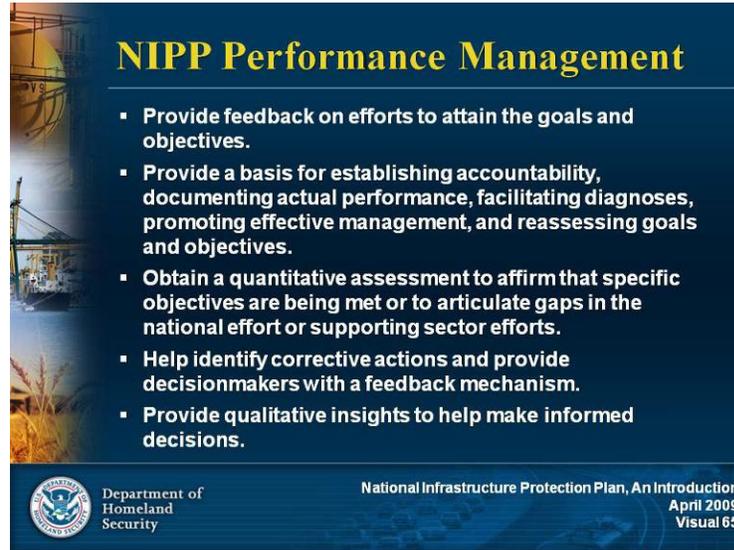
Key Points

While the results of risk analyses help set national and sector priorities, performance metrics allow NIPP partners to track progress against these priorities. The metrics provide a basis to establish accountability, document actual performance, facilitate diagnoses, promote effective management, and provide a feedback mechanism to decisionmakers.



Caption: Graphic showing the role measuring effectiveness plays in the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.

Visual 65



NIPP Performance Management

- Provide feedback on efforts to attain the goals and objectives.
- Provide a basis for establishing accountability, documenting actual performance, facilitating diagnoses, promoting effective management, and reassessing goals and objectives.
- Obtain a quantitative assessment to affirm that specific objectives are being met or to articulate gaps in the national effort or supporting sector efforts.
- Help identify corrective actions and provide decisionmakers with a feedback mechanism.
- Provide qualitative insights to help make informed decisions.

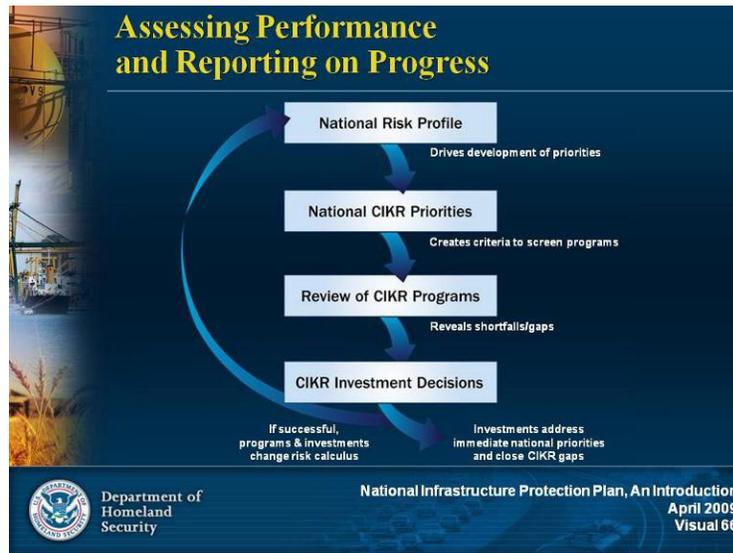
Department of Homeland Security
National Infrastructure Protection Plan, An Introduction
April 2009
Visual 65

Visual Description: NIPP Performance Management

Key Points

The key to NIPP performance management is to align outcome metrics to sector priorities. NIPP metrics are evolving from the current focus on descriptive and output data to a focus on outcome metrics. The next stage of NIPP implementation will concentrate on working with the sectors to identify and track outcome metrics that are aligned to sector priorities and provide NIPP partners with a more comprehensive assessment of the success of CIKR protection efforts.

Visual 66



Visual Description: Assessing Performance and Reporting on Progress

Key Points

- Assessing Performance and Reporting on Progress.** The National CIKR Protection Annual Report is based on information about priorities, requirements, and related program funding information that is submitted to DHS by the SSA of each sector, the SLTTGCC, and the RCCC. The National CIKR Protection Annual Report analyzes information about sector priorities, requirements, and programs in the context of the National Risk Profile, a high-level summary of the aggregate risk and protective status of all sectors.

The National Risk Profile drives the development of national priorities, which, in turn, are used to assess existing CIKR programs and to identify existing gaps or shortfalls in national CIKR protection efforts. This analysis provides the Executive Office of the President with information that supports both strategic and investment decisions related to CIKR protection and resiliency.

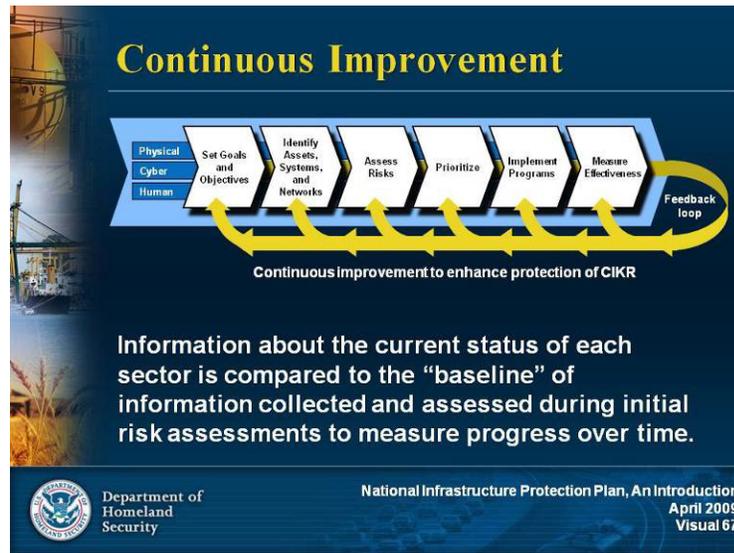
- Qualitative Feedback.** The NIPP provides mechanisms for qualitative feedback that can be applied to augment and improve the effectiveness and efficiency of public- and private sector CIKR protective programs and resiliency strategies.

DHS works with sector partners to identify and share lessons learned and best practices for all aspects of the risk management process. DHS also works with SSAs to share relevant input from partners and other sources that can be used as part of the national effort to continuously improve CIKR protection.



Caption: Graphic showing the process for assessing performance and reporting on progress: National Risk Profile drives development of priorities; National CIKR Priorities creates criteria to screen programs; Review of CIKR Programs reveals shortfalls/gaps; CIKR Investment Decisions address immediate national priorities and close CIKR gaps. If successful, programs and investments change risk calculus.

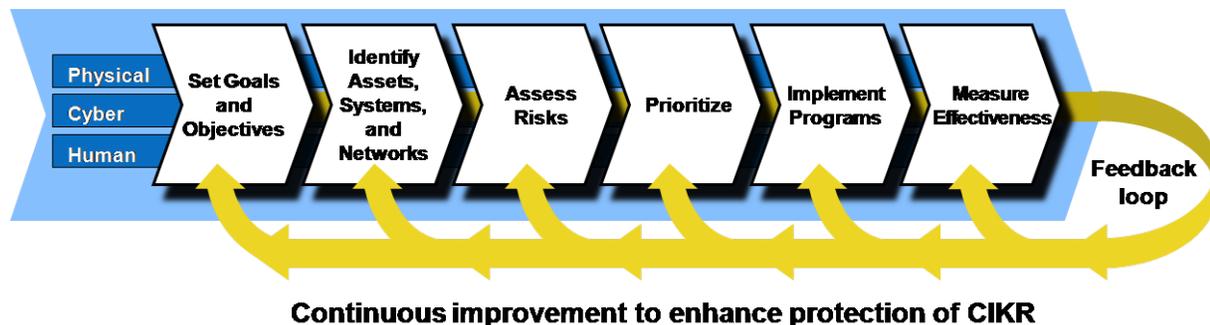
Visual 67



Visual Description: Continuous Improvement

Key Points

By using NIPP metrics to evaluate the effectiveness of efforts to achieve sector priorities, CIKR partners can adjust and adapt their protection approaches to account for progress achieved, as well as changes in the threats of concern. Information about the current status of each sector is compared to the “baseline” of information collected and assessed during initial risk assessments to measure progress over time.



Caption: Graphic showing the role of continuous improvement in the risk management framework.

Visual 68

Sector-Specific Plans (SSPs)

Using the risk management framework, SSPs are:

- Tailored to address the unique perspective and risk landscape of each sector.
- Developed by the SSAs in collaboration with Sector and Government Coordinating Councils and others.

Department of Homeland Security

National Infrastructure Protection Plan, An Introduction
April 2009
Visual 68

Visual Description: Sector-Specific Plans (SSPs)

Key Points

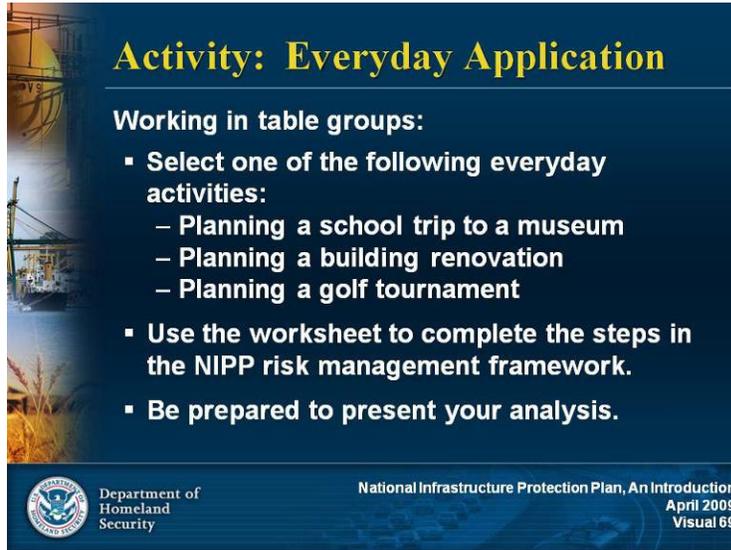
Using the risk management framework, each sector develops an SSP. These plans are:

- Tailored to address the unique perspective and risk landscape, and methodologies and approaches associated with each sector.
- Developed jointly by the SSAs in close collaboration with Sector and Government Coordinating Councils (SCCs and GCCs) and others, including State, local, and tribal CIKR partners with key interests or expertise appropriate to the sector.

Topic

Activity

Visual 69



Activity: Everyday Application

Working in table groups:

- Select one of the following everyday activities:
 - Planning a school trip to a museum
 - Planning a building renovation
 - Planning a golf tournament
- Use the worksheet to complete the steps in the NIPP risk management framework.
- Be prepared to present your analysis.

Department of Homeland Security

National Infrastructure Protection Plan, An Introduction
April 2009
Visual 69

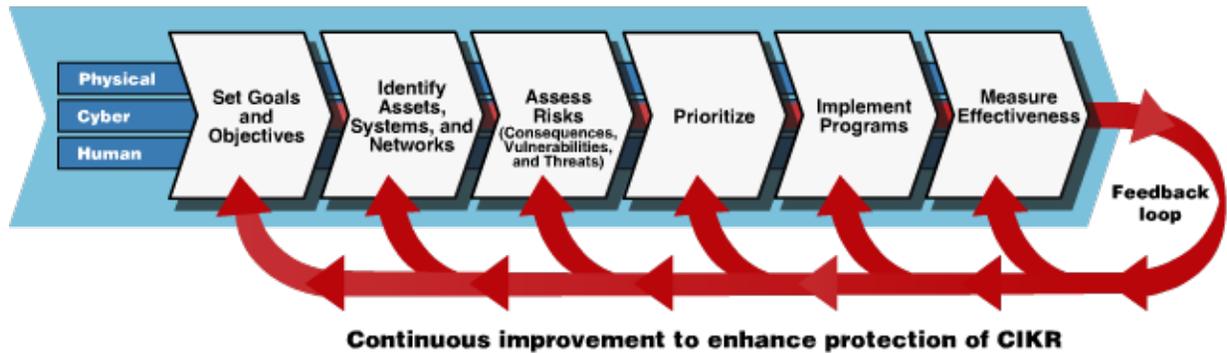
Visual Description: Activity: Everyday Application

Key Points

Work with your table groups to plan one of the following activities:

- A school trip to a museum
- A building renovation
- A golf tournament

Use the worksheet on the next few pages to complete the steps in the NIPP risk management framework, and be prepared to present an analysis of your scenarios.



Instructions: Complete this worksheet for the selected activity.

Step 1: Set Goals and Objectives

What are the specific outcomes, conditions, or performance targets for effective protection?

Step 2: Identify Assets, Systems, and Networks

What are the assets, systems, and networks that comprise the critical infrastructure and key resources? Include physical, cyber/information, and human resources.

Step 3: Assess Risk (to Assets, Systems, and Networks)

What are the likely threats?

What are the vulnerabilities?

What are the consequences?

Step 4: Prioritize

Review the threats, vulnerabilities, and consequences in Step 3. **Circle the top three priorities.**

Step 5: Implement Protective Programs and Resiliency Strategies

What actions will you take to deter threats, mitigate vulnerabilities, or minimize consequences?

Step 6: Measure Effectiveness

How will you know that your risk management actions are working? (What will happen or not happen?)