



University of Dar es Salaam  
Computing Centre



# Technical Management of ICT Infrastructure (TM ICTI)

## Module 4: Corporate IT /IS Security Management



[www.life.se](http://www.life.se)



United Republic of Tanzania  
President's Office  
**PSM**

[www.utumishi.go.tz](http://www.utumishi.go.tz)



[www.spidercenter.org](http://www.spidercenter.org)

Main Partners

Main Sponsor



# Module Objectives

Familiarize with organizational and managerial aspects of information security and operational risks



# Module Outline

1. Introductions to corporate risk and security Management
2. OCTAVE Method
  - ✓ Introduction
  - ✓ Characteristics and principles
  - ✓ Phase 1
  - ✓ Phase 2
  - ✓ Phase 3

# Introductions to corporate risk and security Management



## Risk Model

### Financial Risks

1. Cash Flow exposures
2. Balance sheet exposures
3. Credit rating (WACC)
4. Currency exposures
5. Credit exposures

### Strategic risks:

1. Market Portfolio
2. Customer Portfolio
3. Product & Service Portfolio
4. Supplier Portfolio
5. HR Portfolio

### Hazard risks:

1. Political risks
2. Product extortion
3. Natural disasters
4. NGO

### Operational risks:

1. Business Interruption (due to IT perils, flooding, fire, etc.)
2. Loss of Property (fraud, embezzlement, robbery and theft, kickbacks).

Information security is often one of the operational risks



# Introduction to OCTAVE

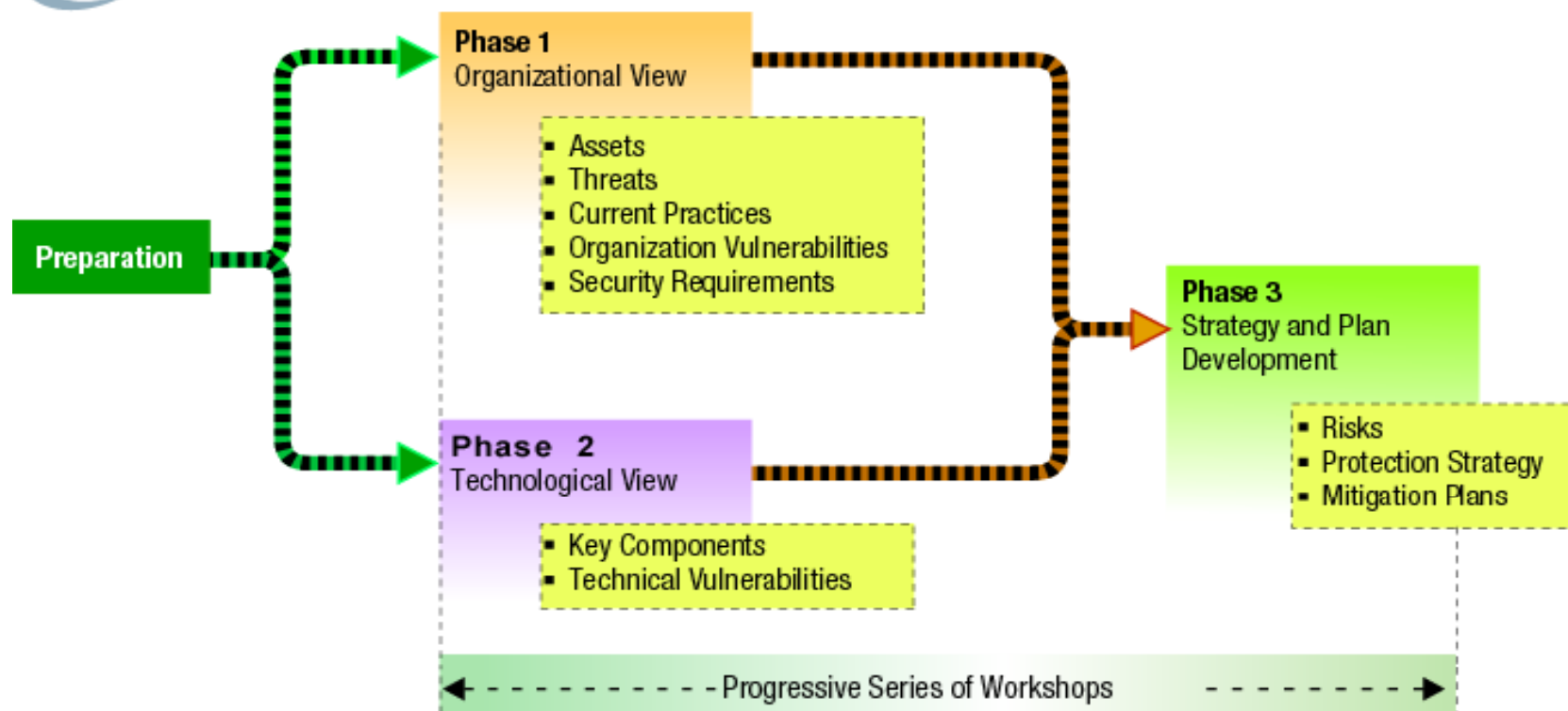
## Definitions

1. OCTAVE - Operationally Critical Threat, Asset and Vulnerability Evaluation
  - **Asset:** Something of value to the organization. E.g. Information, Systems, Software, hardware and People
  - **Threat:** Anything that could harm an ICT asset
  - **Vulnerability:** A deficiency that leaves an asset exposed to harm.
2. OCTAVE is a project method for implementing information security
3. Developed by Software Engineering Institute Carnegie Mellon University and Sponsored by the U.S. Department of Defence

# Introduction to OCTAVE

## Overview

### octave<sup>®</sup> Process





# Introduction to OCTAVE

## Phases and Processes

1. Preparing for OCTAVE
2. Phase 1: Building Asset-Based Threat Profiles
  - ✓ Process 1. Identify Senior Management Knowledge
  - ✓ Process 2. Identify Operational Area Knowledge
  - ✓ Process 3. Identify Staff Knowledge
  - ✓ Process 4. Create Threat Profiles
3. Phase 2: Identify Infrastructure Vulnerabilities
  - ✓ Process 5. Identify Key Components
  - ✓ Process 6. Evaluate Selected Components
4. Phase 3: Develop Security Strategy and Plans
  - ✓ Process 7. Conduct Risk Analysis
  - ✓ Process 8. Develop Protection Strategy



# Introduction to OCTAVE

## Characteristics

**Aself-Directed Method:** A small team of the organization's personnel (Analysis Team) manages the process and analyzes all information.

The basic tasks of the analysis team are to

1. Facilitate the knowledge elicitation workshops of Phase 1
2. Gather any supporting data that are necessary
3. Analyze threat and risk information
4. Develop a protection strategy for the organization
5. Develop mitigation plans to address the risks to the organization's critical assets



# Introduction to OCTAVE

## Characteristics

A workshop-based approach for gathering information and making decisions

1. Workshops are facilitated by the analysis team
2. Participants in the workshops are from multiple organizational levels
3. The result is the identification of
  - ✓ Important information assets
  - ✓ The threats to those assets
  - ✓ The security requirements of the assets
  - ✓ What the organization is currently doing to protect its information assets (current protection strategy)
  - ✓ Weaknesses in organizational policies and practice (organizational vulnerabilities).



# Introduction to OCTAVE

## Characteristics

### Uses Catalogs of Information

1. Catalog of practices - a collection of good strategic and operational security practices
2. Threat profile - the range of threats that an organization needs to consider
3. Catalog of vulnerabilities - a collection of vulnerabilities based on platform and application

An organization conducting OCTAVE benchmarks itself against the above catalogs of information

If an organization must comply with a specific standard of due care, the catalog of practices can be tailored to that standard such as ISO 27001



# Introduction to OCTAVE

## Principles

1. Survivability of the organization's mission .
  - ✓ A key to the success of your organization is achieving your mission, even under adverse conditions.
2. Critical asset-driven threat and risk definition
  - ✓ It is important to focus on critical assets when identifying threats and risks
  - ✓ It is also important to know where to focus your resources
3. Practice-based risk mitigation plans and protection strategy
  - ✓ Mitigation plans and your organization's protection strategy should be based on known, good practices



# Introduction to OCTAVE

## Principles

### 4. Targeted data collection

- ✓ Targeted data collection lets you rapidly reduce the large numbers of items you could be looking at to the **critical few**

### 5. Organization-wide focus

- ✓ Information security risk management has an organization-wide focus
- ✓ It includes senior managers, operational area managers, and staff
- ✓ It covers mission-related areas of the organization as well as the Information Technology department



# Introduction to OCTAVE

## Principles

### 7. Foundation for future security improvement

- ✓ OCTAVE provides you with what you need to get started on what must be a continual focus on security
- ✓ It provides a foundation upon which to build
- ✓ The real information on what's best for your organization will not come from an external expert; it lies within the knowledge and expertise of your own employees and yourself



# Preparing for OCTAVE

## 1. Getting senior management sponsorship

This is the top critical success factor for information security risk evaluations

- ✓ evaluation will require the time of people in the organization
- ✓ The approach that requires staff members from key operational areas, including senior managers
- ✓ If senior managers support the process, people in the organization tend to actively participate
- ✓ If people know that senior management is very interested in the results of the evaluation, then the analysis team will have the authority and backing to convince people to attend the workshops



# Preparing for OCTAVE

## 2. Selecting the analysis team

- ✓ The analysis team is responsible for managing the process and analyzing information
- ✓ The members of the team need to have sufficient skills to lead the evaluation
- ✓ They also need to know when to go outside the team to augment their knowledge and skills



# Preparing for OCTAVE

## 3. Scoping OCTAVE

- ✓ The evaluation should include important operational areas
- ✓ If the scope is too broad, it will be difficult for the analysis team to analyze all of the information
- ✓ If the scope of the evaluation is too small, then the results may not be as meaningful as they should



# Preparing for OCTAVE

## 4. Selecting participants

- ✓ During the knowledge elicitation workshops (Processes 1-3), staff members from multiple organizational levels will contribute their knowledge about the organization
- ✓ It is important for participants to understand their operational areas
- ✓ Participants should be assigned to workshops because of their knowledge and skills, not solely based on who is available. For example Payroll accountant cannot represent the Chief Financial Officer



# Preparing for OCTAVE

## 5. Planning

The goal of planning is to make sure that

- ✓ the evaluation is scoped properly
- ✓ the organisation's senior managers support the evaluation
- ✓ everyone participating in the process understands his or her role and receives any training that is required

The planning activities for OCTAVE start with senior management sponsorship

- ✓ (Where possible) brief the senior management to help them understand the process first!



# Preparing for OCTAVE

## 5. Planning

Select analysis team members

- ✓ Representatives from both the business and information technology parts of the organization will be on the analysis team
- ✓ The size of the analysis team will depend on the size of organisation (OCTAVE suggests 3- 5, but in practise, it depends on the size and structure of the organisation)
- ✓ Senior managers should be involved in the selection of team members
- ✓ In addition, it is helpful if some of the members come from the operational areas that will be participating in the evaluation



# Preparing for OCTAVE

## 5. Planning

Train analysis team

- ✓ The analysis team needs to be trained in the OCTAVE Method
- ✓ Each member of the analysis team needs to understand his or her role during each workshop

Select operational areas to participate in OCTAVE

- ✓ A key part of the planning process is selecting the operational areas that will participate in OCTAVE.
- ✓ This scopes the evaluation
- ✓ Senior managers need to be involved in this activity as well



# Preparing for OCTAVE

## 5. Planning

Select participants

- ✓ Participants for the knowledge elicitation workshops need to be selected
- ✓ people with special skills to augment the analysis team at certain points in the process need to be selected
- ✓ The analysis team members will lead the selection of profiles of participants. They need to get input from the senior managers as well as the managers for each of the operational areas participating in the evaluation



# Preparing for OCTAVE

## 5. Planning

### Coordinate logistics

- ✓ The analysis team members need to ensure that rooms, equipment, and any supporting data are available for all workshops
- ✓ E.g. Enough number of worksheets for all sessions etc
- ✓ Security!

### Brief all participants

- ✓ The analysis team should conduct a briefing for all participants prior to their participation in the process

Once the planning is completed, the organization is ready to start the evaluation process



# Phase 1: Build Asset-Based Threat Profiles

## Organizational Evaluation

To examine key areas of expertise within the organization in order to identify

1. important information assets
2. The threats to those assets
3. The security requirements of the assets
4. What the organization is currently doing to protect its information assets (protection strategy practices)
5. Weaknesses in organizational policies and practice (organizational vulnerabilities).



# Phase 1: Build Asset-Based Threat Profiles

## Process 1: Identify Senior Management Knowledge

To obtain the senior management perspective on

- ✓ Assets
- ✓ Threats to the assets
- ✓ Security requirements of the assets
- ✓ Current protection strategy practices
- ✓ Organizational vulnerabilities

To select or confirm the key operational areas to include in the evaluation

Note: You need to have

- ✓ The organization's policies and procedures
- ✓ An organizational chart
- ✓ Any laws, regulations and standards with which your organization must comply (SOX, EuroSOX, Basel II, Solvency II, ISO 27001, ISO 2000 (ITIL), e.t.c.



# Phase 1: Build Asset-Based Threat Profiles

## Process 1: Identify Senior Management Knowledge

Discuss the objectives and the ultimate results with Senior Management

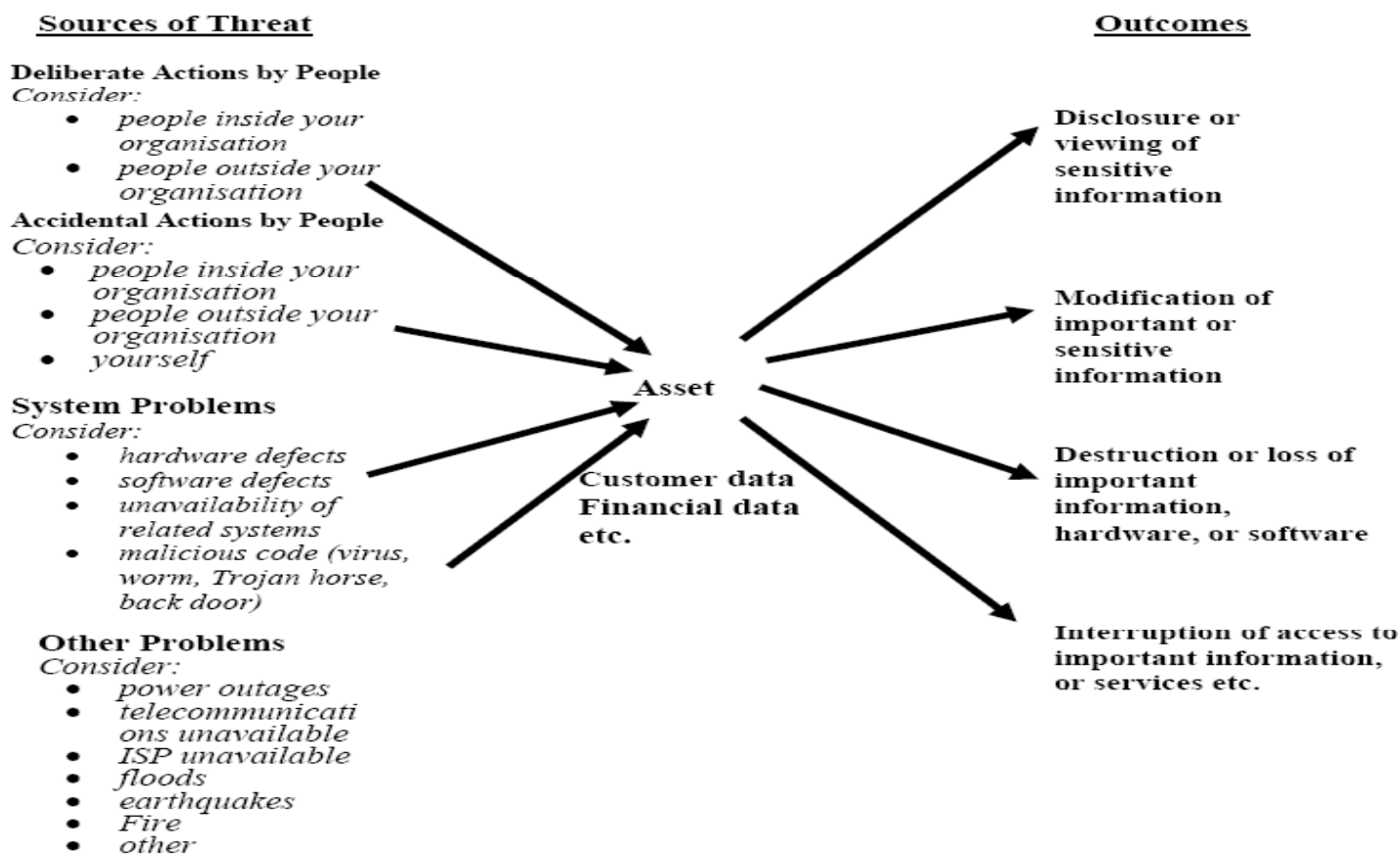
1. Describe for the senior managers what success will look like
2. Indicate that they will be generating the following
  - ✓ A list of assets that are important to the mission of the organization
  - ✓ A list of the five most important assets
  - ✓ A list of scenarios that threaten the most important assets
  - ✓ The security requirements of the most important assets
  - ✓ Current protection strategy practices used by the organization to protect important assets
  - ✓ Organizational vulnerabilities, indicating missing or inadequate protection strategy practices
3. You could also show the worksheets that will be used during the workshop to the managers as you go over the above list



# Phase 1: Build Asset-Based Threat Profiles

## Process 1: Identify Senior Management Knowledge

*What scenarios threaten your important assets?*





# Phase 1: Build Asset-Based Threat Profiles

## At the End of Process 1: Identify Senior Management Knowledge

You should have identified the senior management perspective of

- ✓ Assets
- ✓ Threats to the assets
- ✓ Security requirements of the assets
- ✓ Current protection strategy practices
- ✓ Organizational vulnerabilities



# Phase 1: Build Asset-Based Threat Profiles

## Process 2: Identify Operational Area Management Knowledge

1. To obtain the operational area management perspective on
  - ✓ Assets
  - ✓ Threats to the assets
  - ✓ Security requirements of the assets
  - ✓ Current protection strategy practices
  - ✓ Organizational vulnerabilities
2. To select or confirm the key staff members to include in the evaluation
3. Note: Similar steps except that the focus now is on the operations!



# Phase 1: Build Asset-Based Threat Profiles

## Process 3: Identify Staff Knowledge

1. obtain the staff perspective on
  - ✓ Assets
  - ✓ Threats to the assets
  - ✓ Security requirements of the assets
  - ✓ Current protection strategy practices
  - ✓ Organizational vulnerabilities
2. Note: People who understand the mission of the organization as well as people who maintain the information technology infrastructure play important roles in information security risk assessments



# Phase 1: Build Asset-Based Threat Profiles

## Process 4: Create Threat Profiles

The participants in this process are the core analysis team members as well as any supplemental personnel

The analysis team consolidates the information gathered during Processes 1 through 3, selects few critical assets, and defines the security requirements and threats to those assets

1. Group assets, security requirements, and areas of concern by organizational level
  - ✓ An integrated view of the important information assets, the areas of concern, and the security requirements of the assets are created
2. Select critical assets.
  - ✓ The grouped information is examined and the assets that are most critical to meeting the mission of the organization are identified.
  - ✓ These are known as the critical assets.



# Phase 1: Build Asset-Based Threat Profiles

## Process 4: Create Threat Profiles

1. Refine security requirements for critical assets.
  - ✓ The security requirements for each critical asset are defined.
  - ✓ Any relevant security requirements that were generated during the knowledge elicitation workshops are built upon and refined.
2. Identify threats to critical assets.
  - ✓ A threat profile for each critical asset is built.
  - ✓ Use the basic threat profile as a benchmark to create the range of threat scenarios that affects each critical asset.
  - ✓ If necessary, the basic threat profile is expanded to address new sources of threat.



# Phase 1: Build Asset-Based Threat Profiles

## Process 4: At the end of process

Should have completed the following

1. Selected critical assets
2. Described the security requirements for the critical
3. Assets
4. Identified threats to the critical assets



## Phase 2: Identify Infrastructure Vulnerabilities

### Evaluation of the Information Infrastructure

To examine the key operational components of the information technology infrastructure for weaknesses (technology vulnerabilities) that can lead to unauthorized action

A vulnerability evaluation is a systematic examination of an organization's technology base to

1. Determine the adequacy of the organization's security measures
2. Identify security deficiencies
3. Provide data from which to predict the effectiveness of proposed security measures
4. Confirm the adequacy of security measures after implementation



## Phase 2: Identify Infrastructure Vulnerabilities

### Evaluation of the Information Infrastructure

Technology vulnerabilities can be grouped into the following categories

1. Design vulnerability - a vulnerability that is inherent in the design or specification of the system's hardware or software. Even a perfect implementation of the design may result in a design vulnerability
2. Implementation vulnerability - a vulnerability that occurs from a flawed software or hardware implementation of a satisfactory design
3. Configuration vulnerability - a vulnerability stemming from system configuration or administration errors



## Phase 2: Identify Infrastructure Vulnerabilities

### Process 5: Identify key IT systems and components

identify classes of infrastructure components to examine for technology vulnerabilities

Classes of components are types of devices or systems that are important in processing, storing, or transmitting critical information. The following are the key classes of components to consider:

- ✓ Servers – hosts that provide services to the organization
- ✓ Networking components – Routers, switches, and modems
- ✓ Security components – A firewall
- ✓ Desktop workstations and Laptops
- ✓ Storage
- ✓ Wireless components



## Phase 2: Identify Infrastructure Vulnerabilities

### Process 5: Identify key IT systems and components

select an approach for evaluating each infrastructure component

1. Who will perform the evaluation?
  - ✓ Self
  - ✓ Outsourcing
2. Which tool(s) will be used?
  - ✓ Operating system scanners
  - ✓ Network infrastructure scanners
  - ✓ Specialty, targeted, or hybrid scanners
  - ✓ Checklists
  - ✓ Scripts



## Phase 2: Identify Infrastructure Vulnerabilities

Process 6: Examine systems and components for technology weaknesses

To review technology vulnerabilities with respect to the critical assets and summarize results

1. Reviewing the results of the vulnerability tools
2. Generating a summary of the technology vulnerabilities for selected infrastructure components



# Phase 3: Develop Security Strategy and Plans

## Objectives

1. To analyse the information generated by the organizational and information infrastructure evaluations (Phases 1 and 2):
    - ✓ to identify risks to the enterprise and
    - ✓ to evaluate the risks based on their impact to the organization's mission
  2. To develop a protection strategy for the organization and mitigation plans addressing the highest priority risks
- A risk is essentially a threat plus the resulting impacts to the organization based on
- ✓ Disclosure of a critical asset
  - ✓ Modification of a critical asset
  - ✓ Loss or destruction of a critical asset
  - ✓ Interruption of access to a critical asset



## Phase 3: Develop Security Strategy and Plans

### Process 7: Conduct Risk Analysis

1. To document the information security risks to the organization
2. To create a benchmark against which risks can be evaluated
3. To evaluate the risks to the organization



## Phase 3: Develop Security Strategy and Plans

### Process 8: Develop Protection Strategy

1. To develop a protection strategy for the organization
2. To develop mitigation plans for the risks to the critical assets
3. To develop an action list of near-term actions



## Phase 3: Develop Security Strategy and Plans

### Reviewing Protection Strategy and Risk Information

Review the following information

- ✓ Protection strategy practices
- ✓ Organizational vulnerabilities
- ✓ Technology vulnerabilities
- ✓ Security requirements
- ✓ Risk profiles



## Phase 3: Develop Security Strategy and Plans

### Protection Strategy and Mitigation Plans

The protection strategy and mitigation plans are created

Using

- ✓ Risk profiles for critical assets
- ✓ Areas of concern for critical assets
- ✓ Current practices
- ✓ Organizational vulnerabilities
- ✓ Technology vulnerabilities
- ✓ Catalog of practices

Protection Strategy

1. Provides direction for future information security efforts
2. Defines the strategies that an organization uses to
  - ✓ Enable security
  - ✓ Initiate security
  - ✓ Implement security
  - ✓ Maintain security



## Phase 3: Develop Security Strategy and Plans

### Creating Protection Strategies

Develop a strategy for the strategic practice areas considering

- ✓ The current strategies that your organization should continue to use in each area
- ✓ New strategies that your organization should adopt in each area

Develop a strategy for the operational practice areas considering

- ✓ Training and education initiatives
- ✓ Funding
- ✓ Policies and procedures
- ✓ Roles and responsibilities
- ✓ Collaborating with other organizations and with external experts



## Phase 3: Develop Security Strategy and Plans

### Creating Mitigation Plans

Develop mitigation plans for each critical asset considering

- ✓ Actions to recognize or detect this threat type as it occurs
- ✓ Actions to resist this threat type or prevent it from occurring
- ✓ Actions to recover from this threat type if it occurs
- ✓ Other actions to address this threat type



# Phase 3: Develop Security Strategy and Plans

## Creating an Action List

### Action List

- ✓ Defines the near-term actions that the organization's staff can take
- ✓ Actions on the action list generally don't require specialized training, policy changes, or changes to roles and responsibilities

### Develop an action list considering

- ✓ Near-term actions that need to be taken
- ✓ Who will be responsible for the actions
- ✓ By when the actions need to be addressed
- ✓ Any actions that management needs to take to facilitate this activity



## Phase 3: Develop Security Strategy and Plans

### Presenting the outcome to the Management

1. At the end of this process, the analysis team presents the proposed protection strategy, mitigation plans, and action list to senior managers in the organization
2. The senior managers review and revise the strategy and plans as necessary and then decide how the organization will build on the results of the evaluation



## Phase 3: Develop Security Strategy and Plans

### Presenting the outcome to the Management

The following are proposed

Review risk information

- ✓ The analysis team provides context to the senior managers by providing a summary of the risk profiles for each critical asset
- ✓ They also provide a summary of the results from the protection strategy survey, the current security practices of the organization, and the organizational vulnerabilities

Review and refine protection strategy, mitigation plans, and action list

- ✓ The analysis team presents the protection strategy, risk mitigation plans for the critical assets, and the action list
- ✓ The senior managers review them and revise, change, and add to them as appropriate



## Phase 3: Develop Security Strategy and Plans

### Presenting the outcome to the Management

Create next steps

- ✓ The senior managers decide how they will build on the results of the evaluation and how they can support an ongoing security improvement initiative

After the organization has developed a protection strategy and risk mitigation plans, it is ready to implement them

This completes the OCTAVE process

More Information: <http://www.cert.org/octave/>

End of Module 4