



OCTAVE[®] Allegro Risk Assessment Training

Welcome

***® Operationally Critical Threat, Asset, and
Vulnerability Evaluation and OCTAVE are
service marks of Carnegie Mellon University.***

Sponsored by the U.S. Department of Defense



Software Engineering Institute

Carnegie Mellon University

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

OCTAVE Allegro

© 2019 Carnegie Mellon University

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0487

Software Engineering Institute

Established in 1984

Federally Funded Research and Development Center (FFRDC)

College-level unit of Carnegie Mellon University

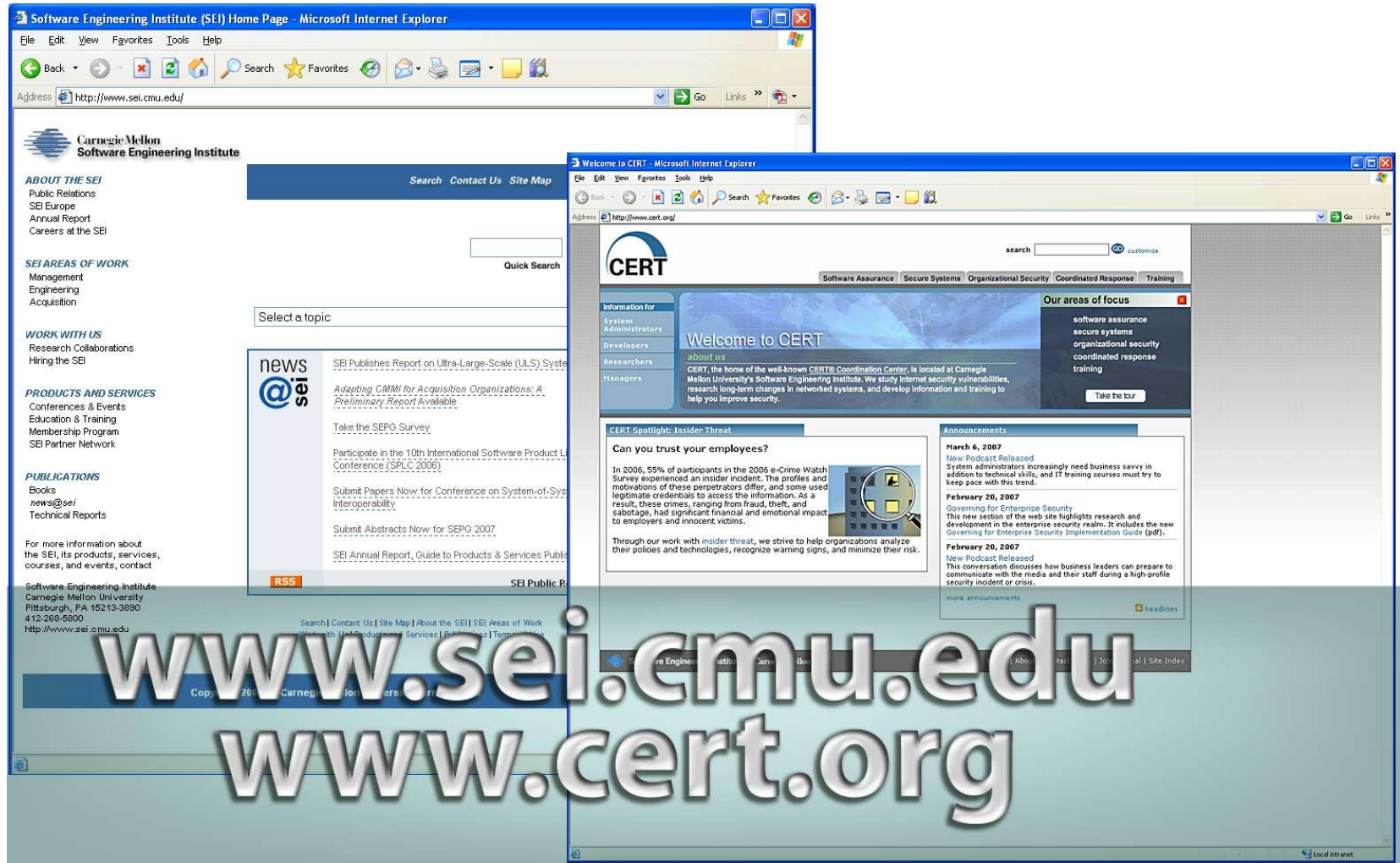
Includes five technical programs aimed helping defense, government, industry, and academic organizations to continually improve software-intensive system

Widely-known “brands”

- CERT Coordination Center
- Capability Maturity Model Integration
 - (CMMI-DEV, CMMI-SVC, CMMI-ACQ)



Visit our Websites



Introductions

Name

Organization and position

Why you are attending this course

Experience conducting risk assessments

Expectations

Logistics



Rules of Conduct

You will be working in teams.

Turn your electronic devices and cell phones to silent.

If you have a question, ask the instructor.

Course Objectives

Have a working knowledge of operational risk, threat, vulnerabilities, impact, services and their related assets

Understand the purpose of the OCTAVE Allegro structured risk assessment approach.

Understand what is required to prepare an organization for a risk assessment using OCTAVE Allegro.

Understand which elements of the various OCTAVE approaches are applicable to your organizations.

Mentor you as you perform a risk assessment using OCTAVE Allegro.

Training Schedule

Day 1

- Introduction and Overview
- Step 1 – Establish Risk Measurement Criteria
- Step 2 – Develop an Information Asset Profile

Day 2

- Step 3 – Identify Information Asset Containers
- Step 4 – Identify Areas of Concern
- Step 5 – Identify Threat Scenarios
- Step 6 – Identify Risks

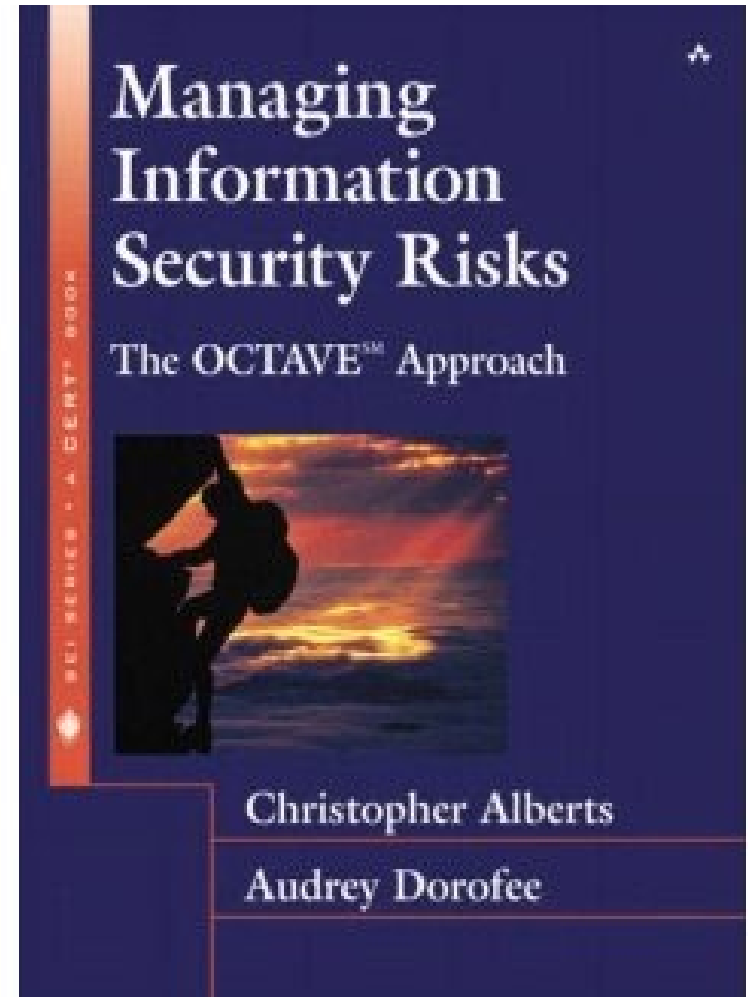
Day 3

- Step 7 – Analyze Risks
- Step 8 – Select Response Approaches
- Summary and Next Steps

Training Materials

The course makes use of the following

- Training slides – student notebook
- Exercises and case studies
- Additional handouts
- *Managing Information Security Risks using OCTAVE* book
- CD-ROM containing additional materials



At the End of This Training...

You will be

- Able to begin the preparation process for conducting a risk assessment using OCTAVE Allegro
- Familiar with the risk management process and how OCTAVE Allegro fits into that larger process

You will understand what, if anything, needs to be tailored.

As you go through this class, mark or otherwise tag anything you think might require tailoring for your organization.

Exercise

In your teams, discuss and define the following words:

- *Information Security*
- *Risk*
- *Risk Management*

Using the flip charts, record your definitions to each of the words.

If you cannot agree on a single definition for a word, write all of the definitions on the flipchart.

Questions and Discussion



Module 2

Risk and Resilience

Overview

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0487

Organizational certainties

Risk environment will not contract – number of risks and complexity will increase.

Organizations must get better at “surviving” in uncertainty.

Knowledge and awareness of risk issues must be pervasive throughout the organization.

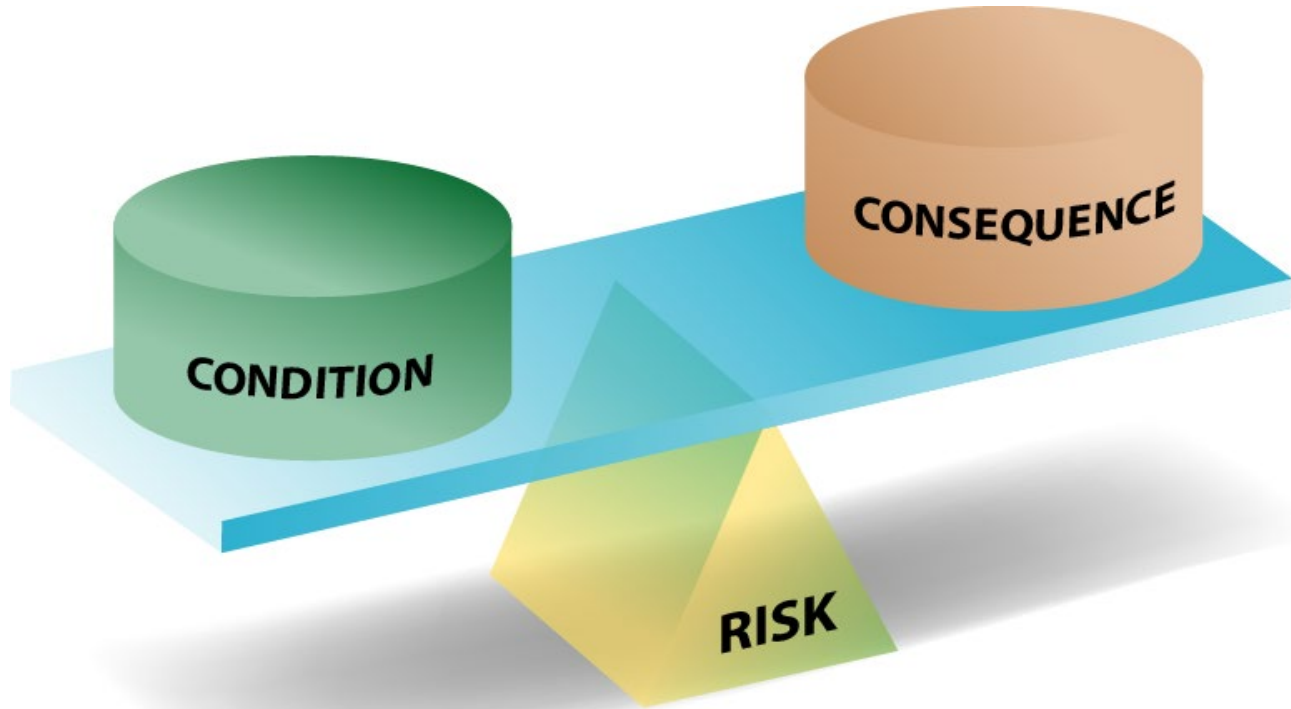
Traditional tools, techniques, and methods may not work in this environment.

Existing organizational structures may not be agile enough to adapt.

Words matter. . .



The basic risk equation



$$\text{RISK} = \text{CONDITION} + \text{CONSEQUENCE}$$

Elements of the risk equation

Condition

- Weakness, exposure, or vulnerability
- Actor
- Motive
- Outcome

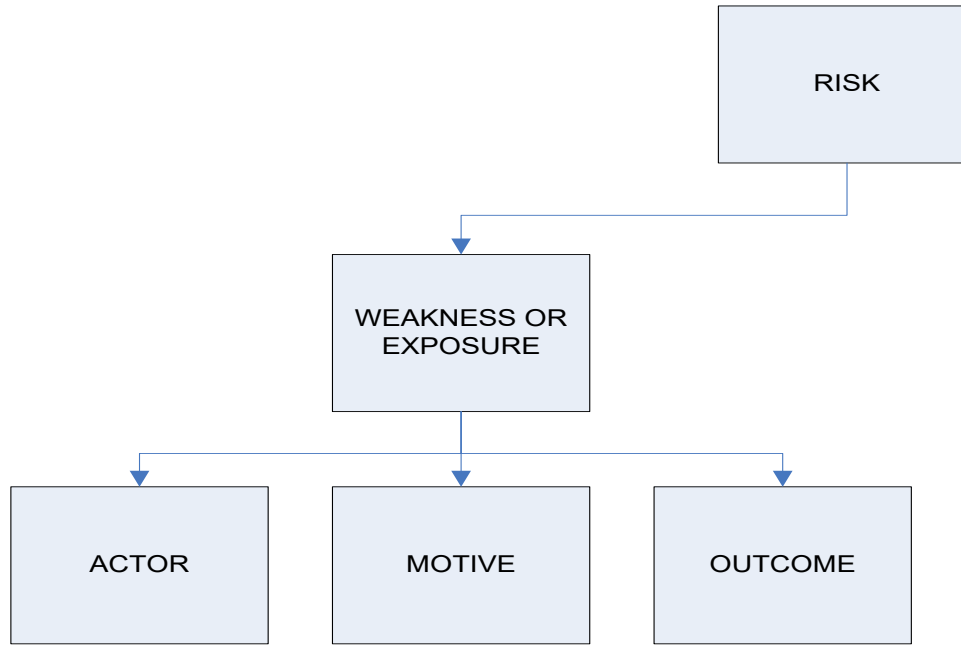
Consequence

- Impact

Uncertainty

- Probability

Assembling the risk elements



Definition of “threat” or “condition”



Impact

An influence or effect

The expected (or realized) result from the *exploitation* of a **threat** and an undesired **outcome**

Often couched in terms of “organizational impact” in various areas:

- Reputation, customer confidence
- Health, safety, and welfare
- Lost productivity
- Lost revenue or sales
- Fines and legal penalties

Typically referred to as the “consequences” of realized risk

Outcome vs. Consequences

Outcome refers to the unwanted or unintended results of an actor with a motive exploiting a weakness, exposure, or vulnerability

Examples:

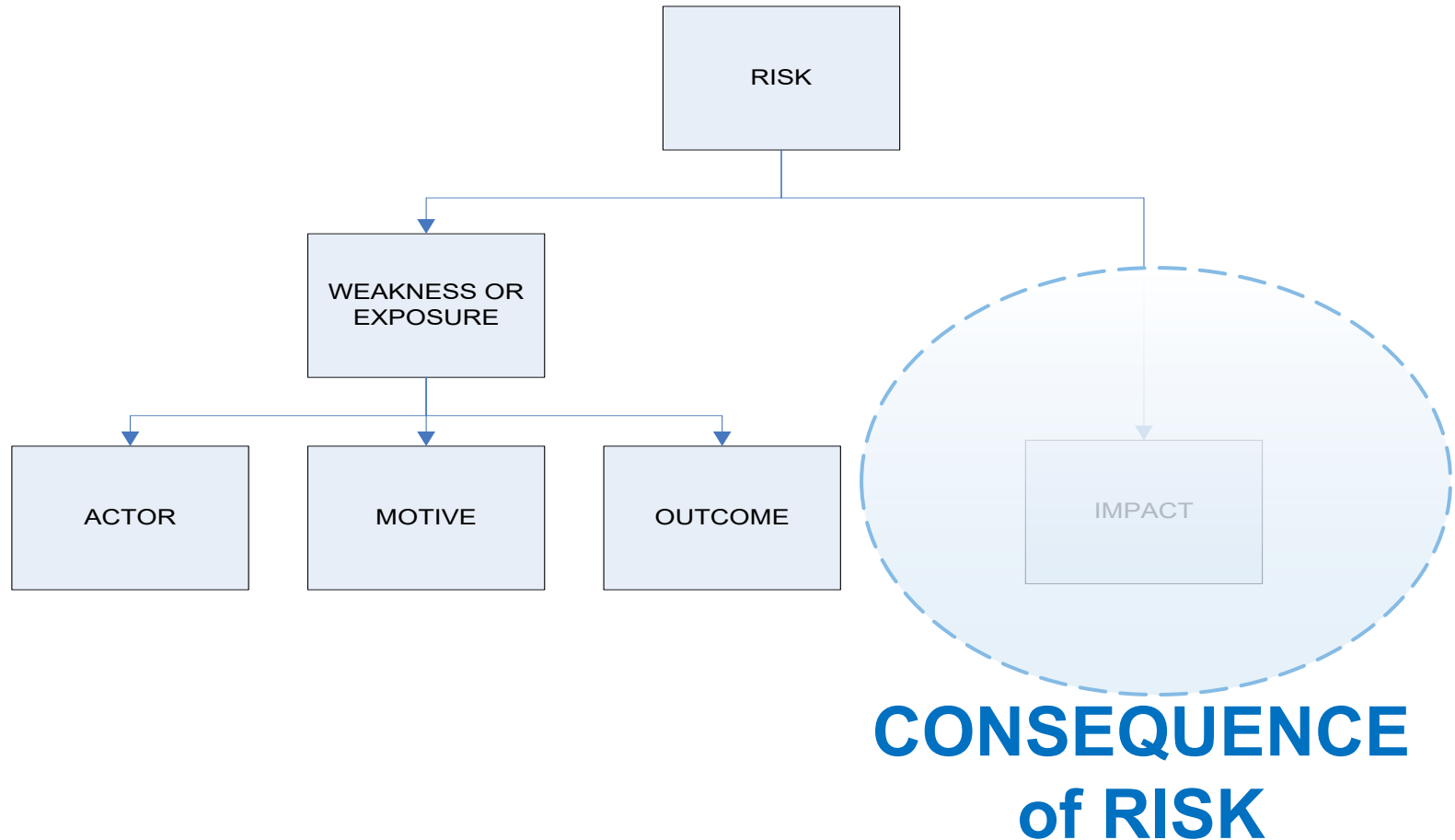
- Access to email or critical systems is denied
- Network is slow; users can't access Internet
- Customers can't place orders on web site
- Remote sensors shut down on gas valves causing explosion

Consequence refers to the impact on a person or organization as a result of the exploitation

Examples:

- Loss of \$50,000 in revenue per hour
- Productivity loss of 45% resulting in \$500,000 of rework
- Reputational damage due to news coverage
- Fine of \$1,000,000
- Loss of life for 20 employees

Positioning “impact” in risk



RISK = CONDITION + CONSEQUENCE

Uncertainty

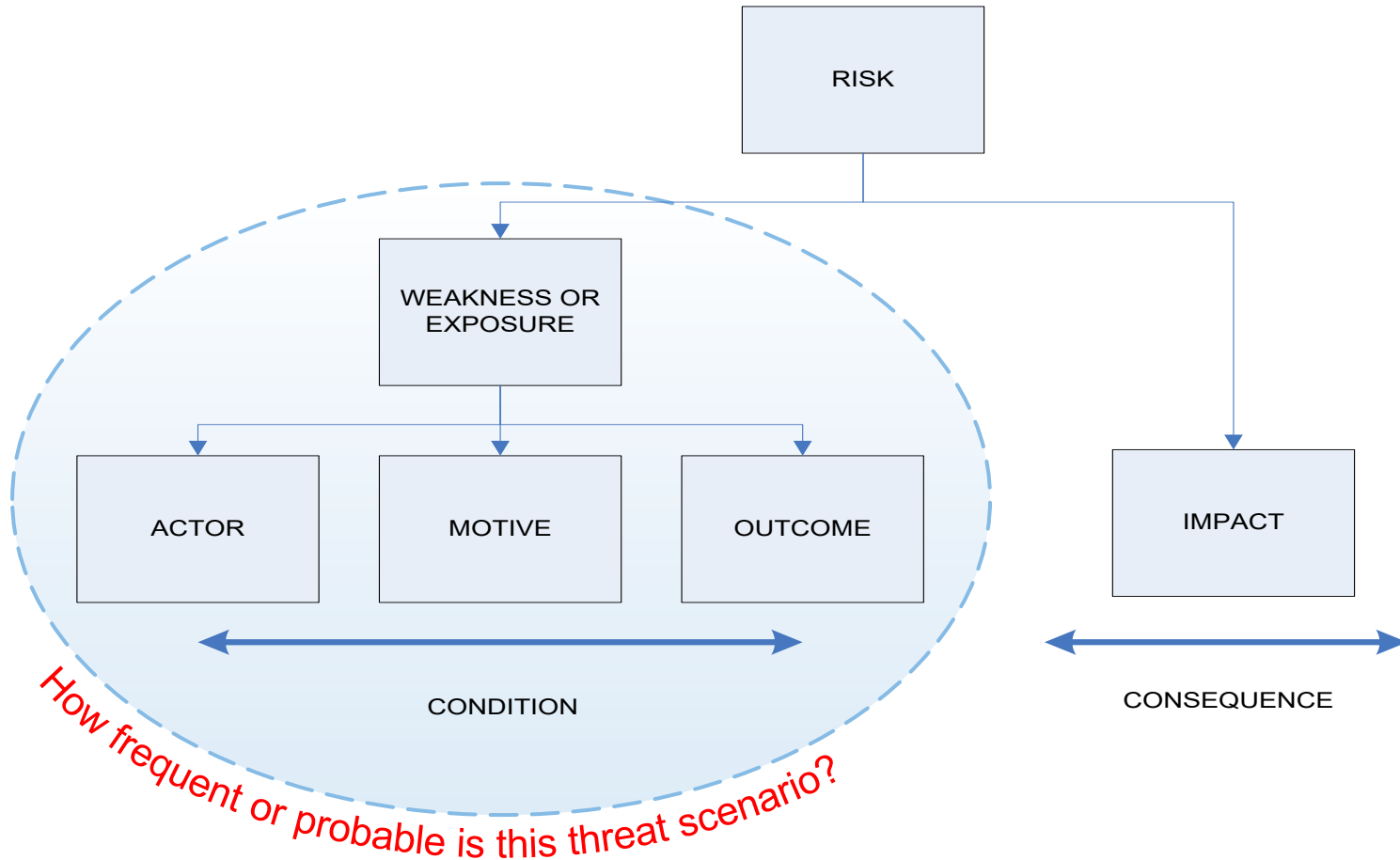
Likelihood or chance of something

Expressed in terms of **probability**

Likelihood that the **threat** or **condition** can be exploited, resulting in

- unwanted **outcomes** that
- result in **impact** or **consequences**

Adding uncertainty



RISK = CONDITION + CONSEQUENCE

Risk and resilience

Resilience is related directly to risk.

The ability to identify and respond to operational risk affects operational resilience.

Why?

- Known risk is addressed before it becomes disruptive.
- Organization is able to make informed decisions about the sustainment of services and assets under uncertain conditions (i.e., unknown risks).

Poor risk management may make the organization less agile, flexible, survivable because the exposure to disruptive conditions is increased.

Challenges for the Organization

Meet mission *no matter what*

Cope with operational risk and minimize impact

Move all operational risk management activities in the same direction

Optimize cost-effectiveness

Find meaningful ways to measure performance



Why do risks matter?

Trust and confidence of employees and customers

Reputation and image

Regulatory compliance, fines, legal penalties

Customer retention and growth

Life, safety, and health of customers and employees

Productivity and profitability

Organizational survival

Definitions

Vulnerabilities

Threats

Control

Vulnerability

A potential exposure or weakness that could be exploited.

The susceptibility of an organizational service or asset to disruption.

Examples are:

- Software
- Hardware
- Physical structures

Threats

A situation, vulnerability, or condition that can be exploited to produce an unexpected or unwanted outcome for the organization.

Origin of threats

Organizational and operational vulnerabilities

Technical vulnerabilities

Environment

External events

People

Properties of a threat

Actor (human or natural)

Motive (accidental or deliberate)

Access or Means (technical, physical)

Undesirable outcome (disclosure, modification, destruction or loss, interruption)

Outcomes of threats

Disclosure or viewing of sensitive information

Modification of important or sensitive information

Destruction or loss of important information, hardware, or software, facilities, or the unavailability of people to do the job

Interruption of access to important information, software, applications, or services

Threat is a part of risk

A threat possesses the means, motive, and opportunity to exploit a weakness or vulnerability.

- Can be a circumstance or event

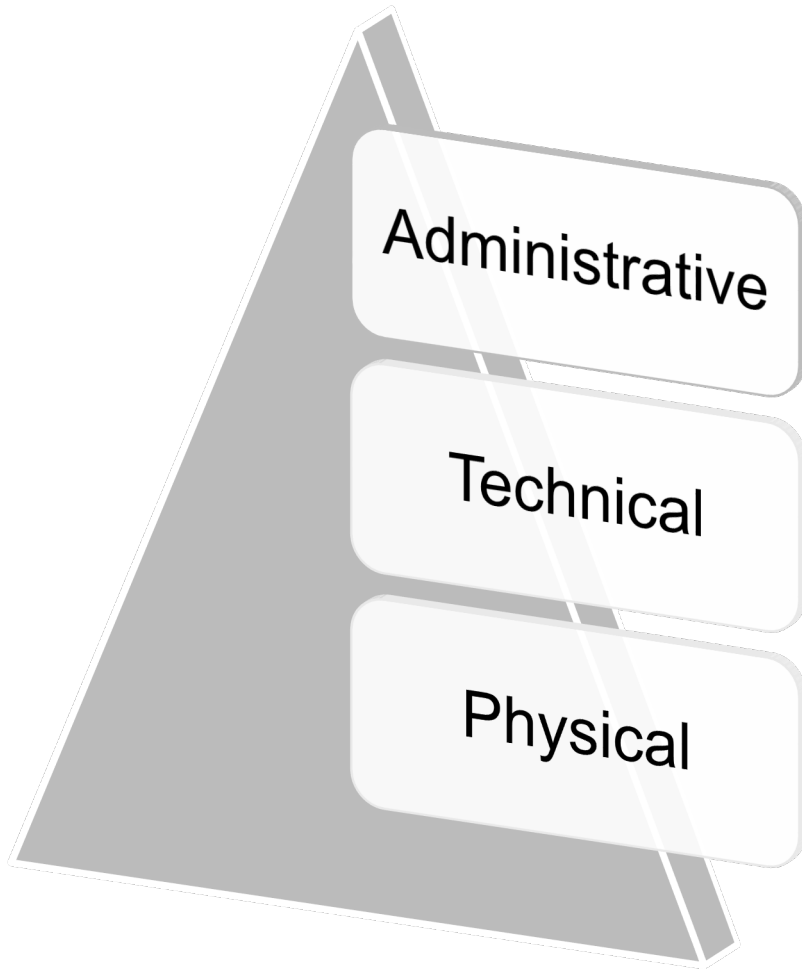
Threat describes the “condition” part of the risk equation.

Risk may not be present if there is no threat present (i.e., there is no vulnerability to exploit).

Control

Policy, procedure, method, tool, technology that the organization uses to meet its objectives

Types of controls



Administrative controls

- Policy, procedures

Technical controls

- Access Control Lists, firewalls

Physical controls

- Physical barriers, access card readers

Layered controls = Defense-in-depth

Controls typically must be layered to provide adequate asset protection and to implement protection strategies.

Example: protect paper medical record

Administrative controls:

- Policy enacting HIPAA regulations
- Limitations on personnel who must handle medical records
- Clean desk policy

Technical controls:

- Bar-code scanning librarian system for checking out records

Physical controls:

- Card reader system for file room where records are stored

Definitions

Risk Assessment

Business Impact Analysis

Risk Management

Risk Assessment (a.k.a. Risk Analysis)

A risk management process focused on understanding the condition and consequences of risk, prioritizing risks, and determining a path for addressing risks.

Determines the importance of each identified operational risk and is used to facilitate the organization's risk disposition and mitigation activities.

Business Impact Analysis

Similar to a risk assessment.

Identified risks are evaluated and analyzed to understand the 'impact' to the organization if the risk should be realized.

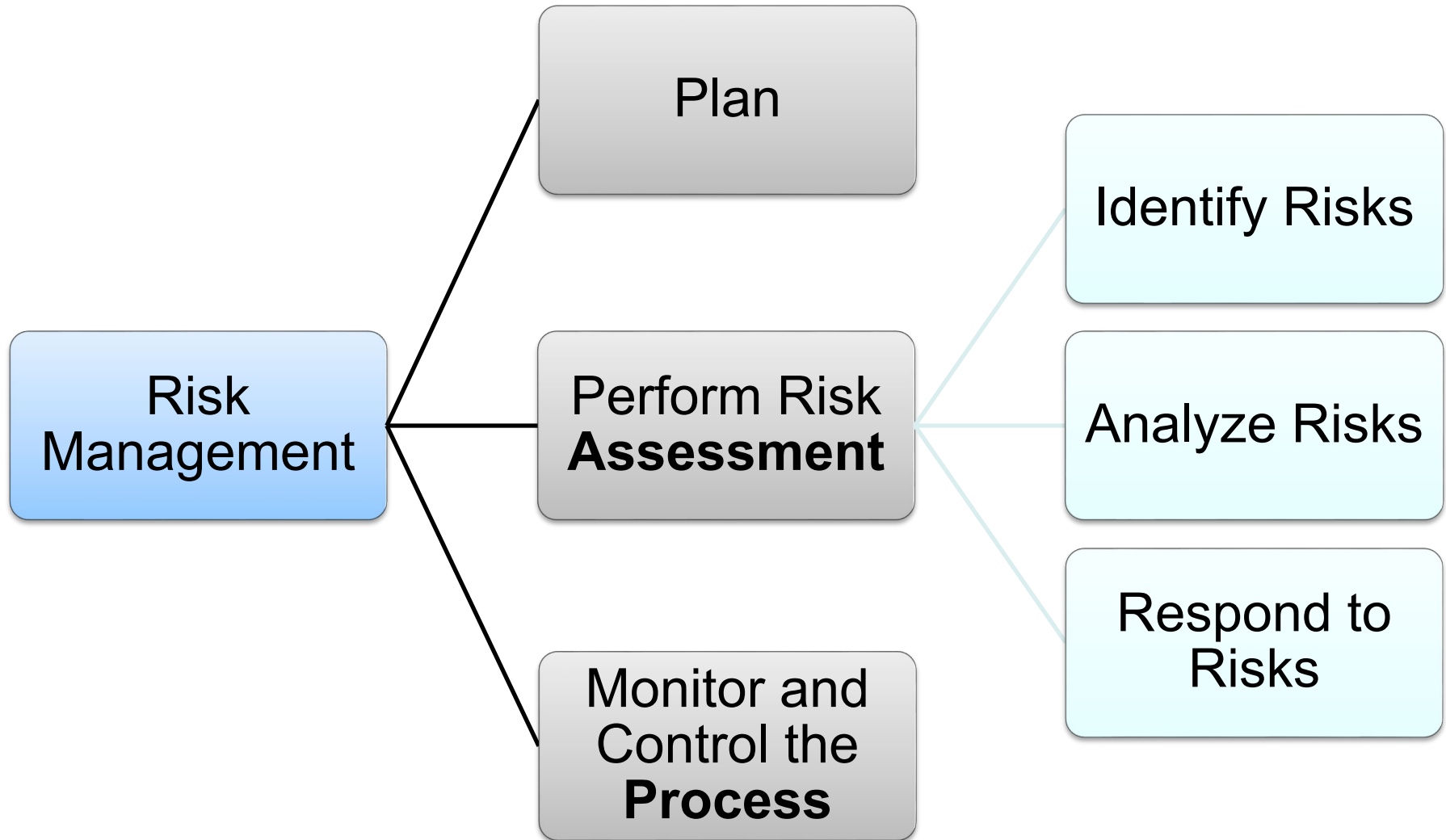
Often very detailed and specific scenarios are considered in a BIA.

Primarily used as part of the planning for Business Continuity or Disaster Recovery.

Risk Management

The continuous process of identifying, analyzing, and responding to risks to organizational assets that could adversely affect the operation and delivery of services.

Risk Management vs. Risk Assessment



Considerations for a Risk Management Program

Basic principles of risk management -1

Cultural and Organizational principles set the foundation for a continuous process

- Open communication
- Global perspective
- Teamwork and collaboration towards a common set of goals

Basic principles of risk management -2

Forward-looking view

Defined, consistent, repeatable process

Focus on the critical few

Integrated into existing management activities

Definitions

Risk management – The overarching program (principles, framework, process) of coordinated activities used to manage risk effectively.

Managing risk – Applying the program activities to specific risks.

Risk appetite and risk tolerance

Risk appetite – The amount of risk an organization is willing to take in pursuit of its strategic objectives

- Example: We will hire 8 people to expand the customer service call center to have people available to take calls until 11pm eastern time.

Risk tolerance – The thresholds that define the risk appetite

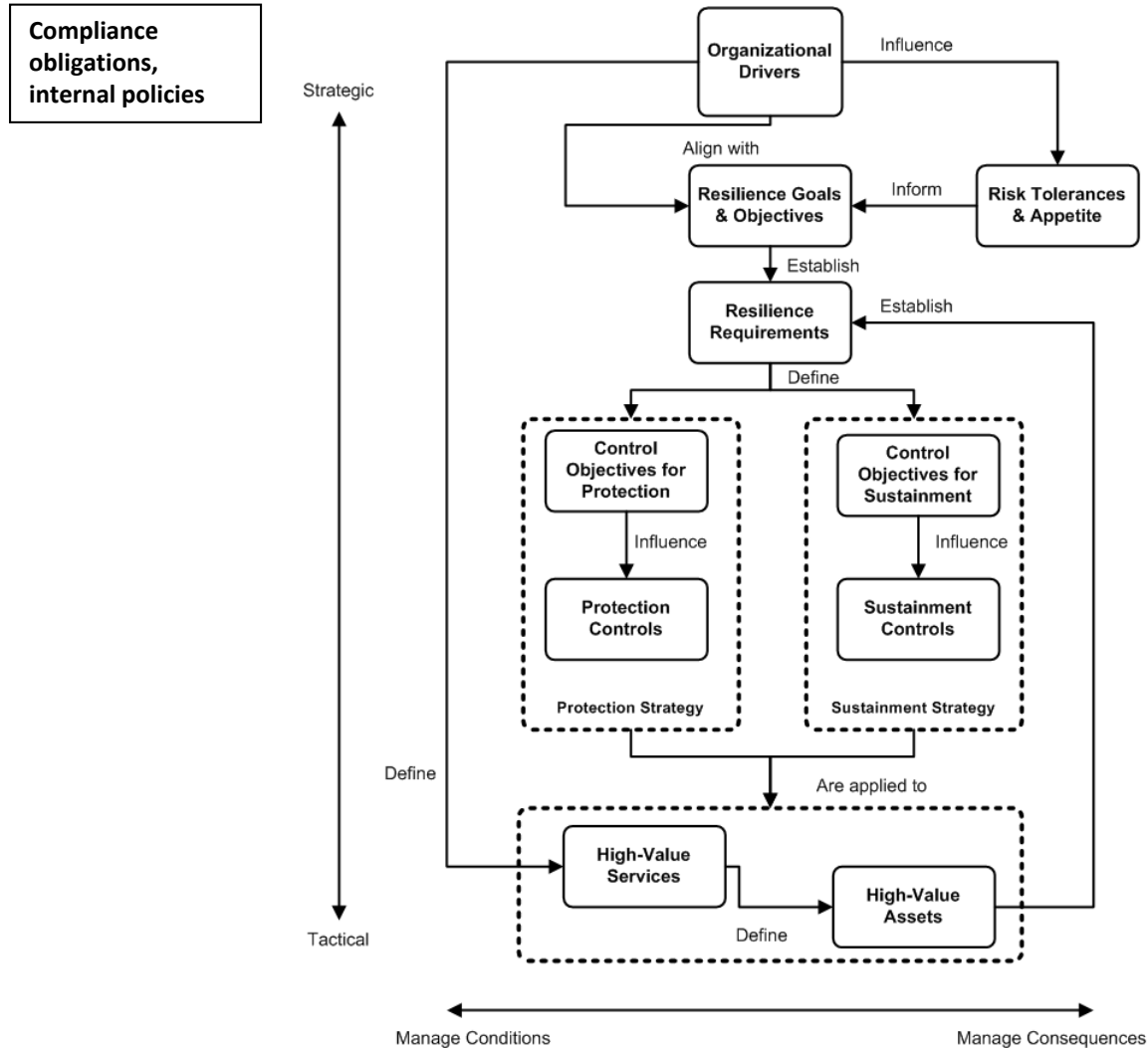
- Example: The minimum number of people we can hire to achieve the objective is 6 and the maximum number is 10.

Key risk indicators

Job descriptions – If the job is not defined accurately, the HR dept. will hire someone with the wrong skills for the job

Training – If the new staff is not given the correct training for the job the risk is that the staff will not be able to satisfy the customer requests

Driving Operational Resilience through Alignment



Challenges to risk management

Disparate risk types

Measurement

Clearly defining the risk appetite and risk tolerances

Competing priorities

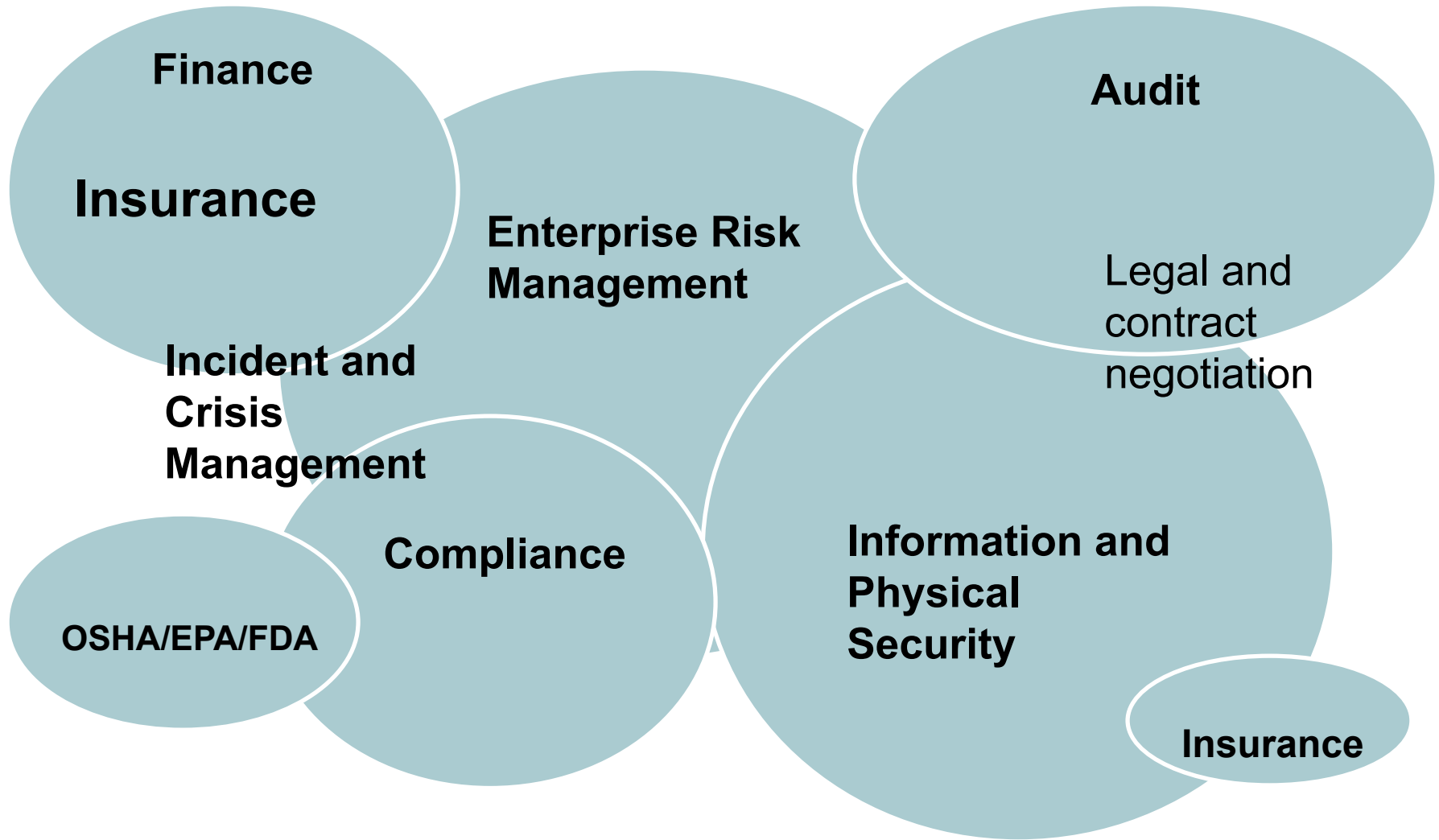
Balancing regulatory view and business view

Ensuring both infrastructure investment and business investment

Internal governance overlap

Risk Alignment and Coordination

Risk areas are often managed independently



Enterprise risk management (ERM)

An activity that looks across all types of **risk activities** in the organization and considers all **risk types**

Not simply an aggregation of individual types of risk – but a process of managing these risks with a view to their interdependencies

Connects risk management to strategic and operational drivers



ERM and ORM



Operational risk management (ORM) is a (significant) subset of ERM.

ORM addresses day-to-day risks that can affect the organization's ability to carry out its mission.

Failure to manage operational risk can have significant impact on the organization's ERM process.

Causes of misalignment in managing operational risks

Organizational risk assumptions are not known or well-communicated

Security and business continuity activities are based on external influences (regulations, laws)

Security, business continuity, and IT operations support operational resilience but risk management activities are performed in silos

Security is the domain of IT and often seen as a technical issue

Business Continuity Impact analysis often assumes total loss/worst case data to calculate protection needs

Requirement: Consistent risk drivers

Risk Management approach is founded on common risk drivers.

Organizational risk tolerance and appetite is part of the organizational culture – “it is the way we do business.”

Security and business continuity activities operate on the same risk assumptions.

If everyone in the organization acts on different risk assumptions, can the organization manage risk effectively?

Requirement: Strategic focus

If all of the organization's activities are not focused on the same strategic objectives, can they be accomplished?

Strategic objectives drive resilience requirements and control objectives.

Resilience activities support and enable the achievement of strategic objectives.

Mission-focus becomes the foundation for managing operational risk to increase resilience.

Requirement: Drive out cost and redundancy

Elimination of silos results in less duplication of effort

Resources are directed to the processes that need the most attention

Cost of risk management is a function of process achievement, not departmental goals or budgets

Costs are controlled by measurement, not event or conjecture

Can you drive out cost and improve effectiveness if you don't know what your current effort costs or how effective it is?

Requirement: Information on progress

Measuring achievement is a means for expressing competency and capability

Provides a better predictor of the organization's ability to manage risk

Progress is expressed in terms of achievement, not in the absence of event or incident

How do you answer the question: Are we secure?

How do you answer the question: Are we resilient?

Do you answer these questions in the absence of relevant data or information?

Resilient organizations. . .

Are agile and capable

Risk management and risk awareness is a way of life

Respond to disruptions instead of reacting

Change before they need to

Sense, respond, thrive, *and improve*

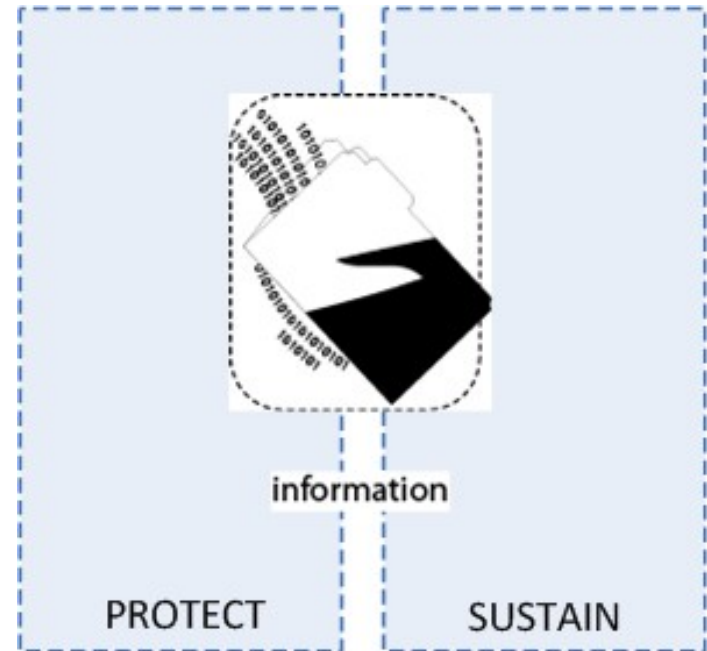
Use security, IT Ops, and business continuity as a means to control, manage, and enable the business.

So What Does This Have To Do With Risk Management?

Asset view

To ensure that **services meet their mission**, related assets must be

- Protected from threats and risks that could disable them
- Continue to sustain operations in a degraded state or under adverse conditions



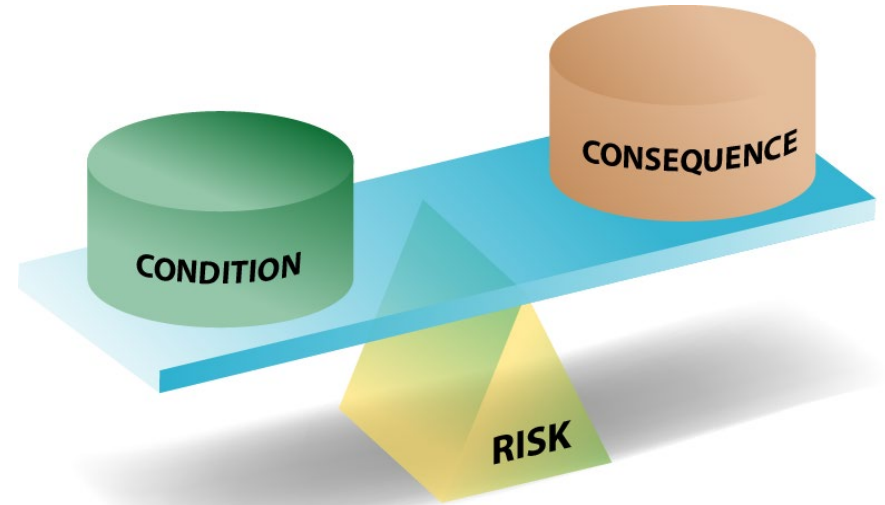
Security is an Op Risk Management activity

Managing firewall rule-sets

Access controls to systems and facilities

Limiting access to intellectual property or confidential information

Confirming identity and privileges



The aim of these “security” activities is ultimately to manage operational risk.

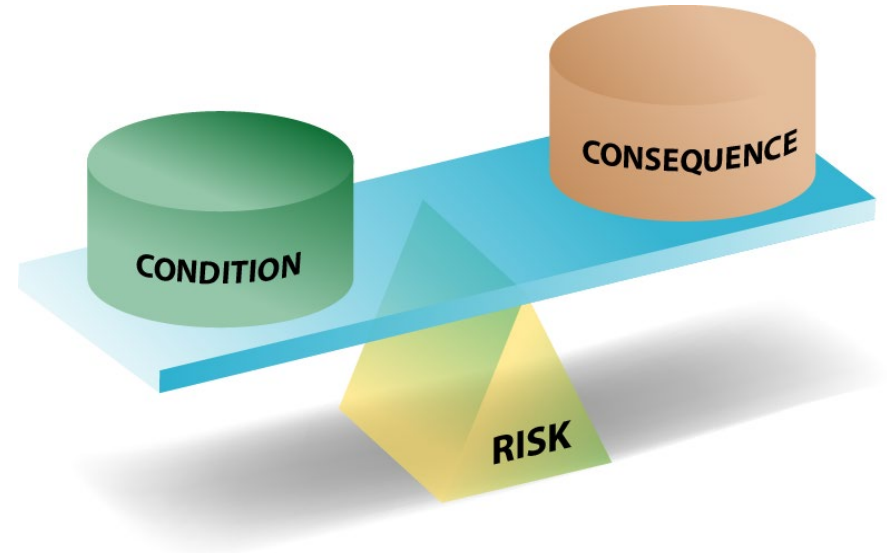
Business Continuity and Disaster Recovery are Op Risk Management activities

Limit unwanted effects of realized risk

Ensure availability and recoverability

Developing business continuity and disaster recovery plans

Manage impact from realized risk



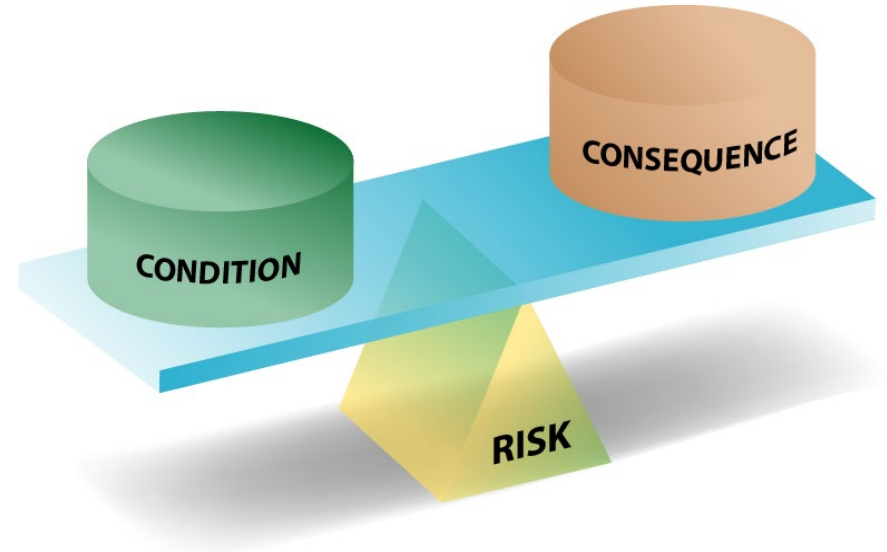
The aim of these “continuity” activities is also to manage operational risk.

IT Operations is an Op Risk Mgmt. activity

Limit vulnerabilities and threats that originate in the technical infrastructure

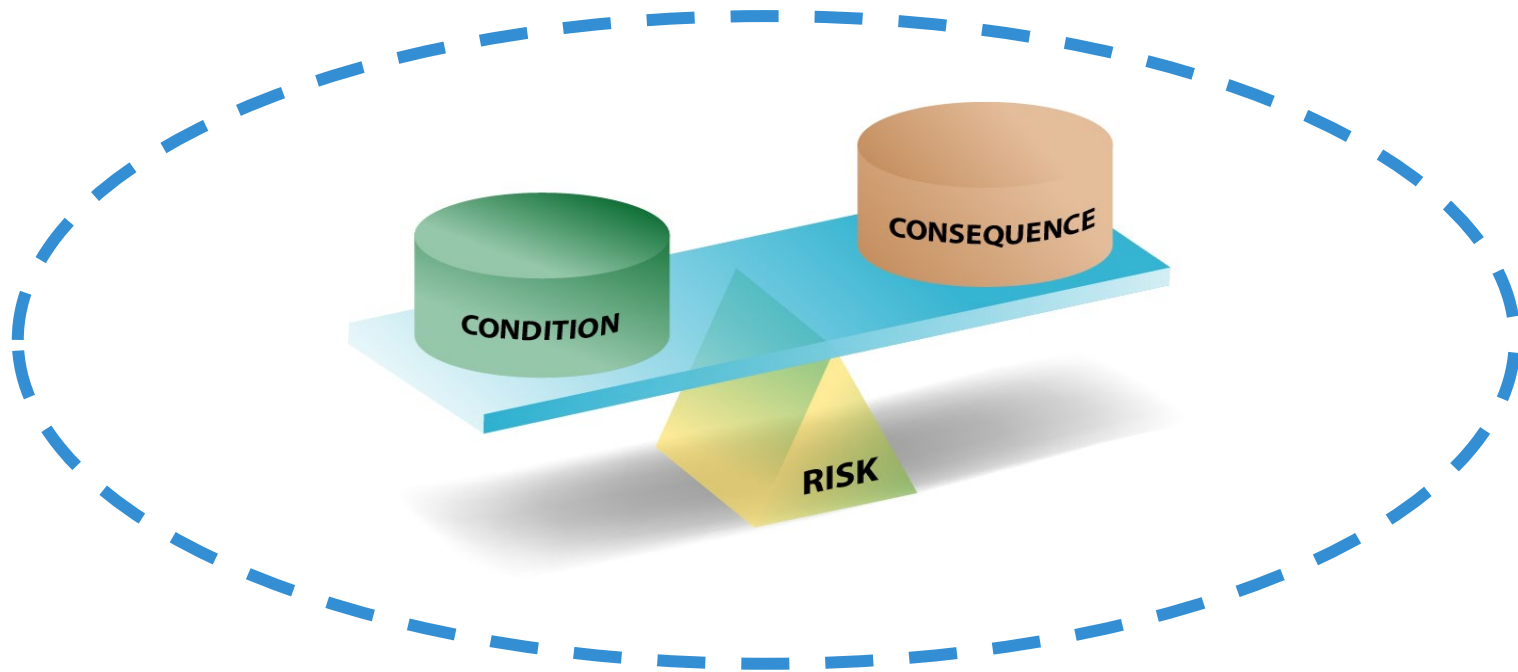
Providing appropriate access to systems & applications for staff and external entities

Ensure availability and recoverability of systems and technology



The aim of these “operations” activities is to manage operational risk.

Managing Operational Risk requires a holistic approach



Managing both sides of the risk equation in alignment with business drivers and full knowledge of costs increases the risk management capability of the organization.

Auditing vs. risk management

Looking back vs. looking forward

Diagnostics – Two kinds

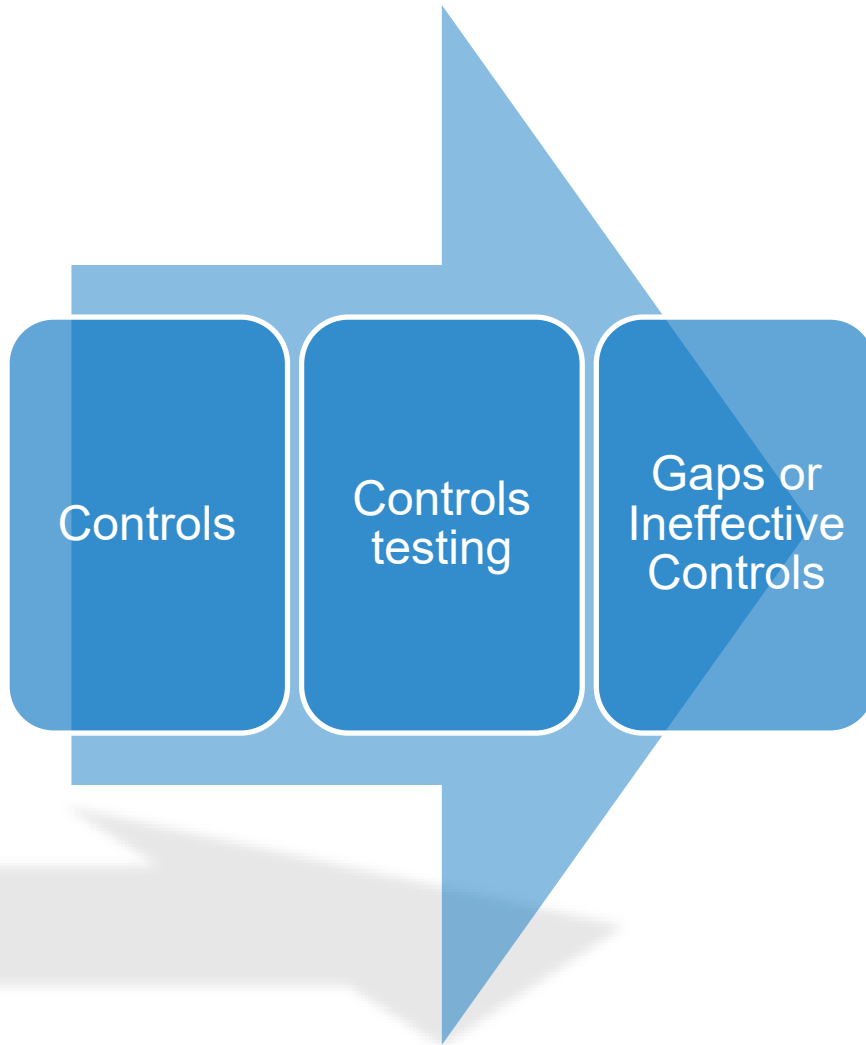
Compliance Based:

- Focused on conformity to a set of criteria
- Focuses on whether the control is present/absent
- Deviation from the criteria creates “findings”

Risk Based:

- Focused on the mission, business processes, and high-value assets
- Standard risk evaluation criteria provides a way to prioritize resources
- Information uncovered creates “risk items”
- If managed well, establishes a broader benchmark of success

From controls to compliance



Controls are selected or inherited or mandated (regulations)

Much time is spent testing and validating controls

Gaps in controls or ineffective controls are remediated (or not)

The Need for a Better Approach to Manage Risk

Current Approaches to Security Management

Security by **compliance**

- FISMA
- HIPAA
- PCI



Security by adoption of **best practices**

- ISO 27000
- DISA STIGs
- Vendor guides



Result

- Uneven use of limited resources

Doing vs. managing

Most organizations have experience at the tactical level

- Significant body of **codes of practices** to guide effort
- Significant range of **technology solutions**
- Practitioners' **skill levels** have matured significantly

BUT – very few organizations are skilled at **managing the process** so that it

- is effective, efficient, optimal, and meets stated objectives
- can produce reliable and predictable results:
 - now (in the steady state)
 - under times of stress
 - under uncertain conditions
 - when the risk environment changes

Technology-centric approaches

Fail to recognize that managing operational risk is an organizational problem

Can be ineffective if they are not actively managed and continuously improved

Often leave management to ask:
“If we have state-of-the-art technologies deployed, why do we still suffer disruptions?”



Vulnerability vs. Risk assessment

Vulnerability assessment is a means to identify threats: weaknesses, exposures, and vulnerabilities

Examples:

- Running automated assessment tools
- Comparing against a threat catalog
- Doing penetration tests

Risk assessment is a process of identifying risks relative to threat; includes probability, impact, and consequence

Examples:

- OCTAVE
- CRAM
- FRAP

Vulnerability assessment is NOT equal to risk assessment.

Types of Risk Assessments

Quantitative

Qualitative

Quantitative Risk Assessment

Assigns “values” to components of risk

Focuses on statistical representation – history, experience, knowledge

Difficult to use when events are unknown or catastrophic

Probability is a major component – characterizing uncertainty in quantitative terms

Qualitative Risk Assessment

Scenario-based

Driven by data collection

Relies upon qualitative criteria to measure risk

Imparts significant judgment into the process – any probability will not be based on mathematical foundations

Often relies on some aspect of quantitative analysis

Common Risk Management Methods

CRAMM – CCTA Risk Analysis and Management Method

- UK government's preferred risk analysis method. Appropriate for large organizations, like government bodies and industry.

ISO27005& ISO31000 – International Organization for Standardization (replaces AS/NZS 4360:2004)

- ISO27005 – Information Security Risk Management
- ISO31010 – Risk Assessment techniques

FRAP – Facilitated Risk Assessment Process

NIST 800-30/NIST 800-39

- Guidance and identification of what should be considered within a risk management and risk assessment approach

OCTAVE – CERT's Operationally Critical Threat, Asset, and Vulnerability Evaluation

Others

NIST 800-30

National Institute of Standards and Technology

Provides a 9-step process for assessing risks to IT systems

More framework, less method

Describes what should be done, but not how

Provides some taxonomy to help you get started

Typically requires a methodology (like OCTAVE) to satisfy the 9 steps

NIST 800-39

National Institute of Standards and Technology

OCTAVE

Developed by Carnegie Mellon's CERT program at the Software Engineering Institute (www.cert.org/resilience)

Asset-focused

Business-oriented and self-directed

Led by a multi-disciplinary analysis team

Comes in three “flavors”: standard, OCTAVE-S and OCTAVE-Allegro

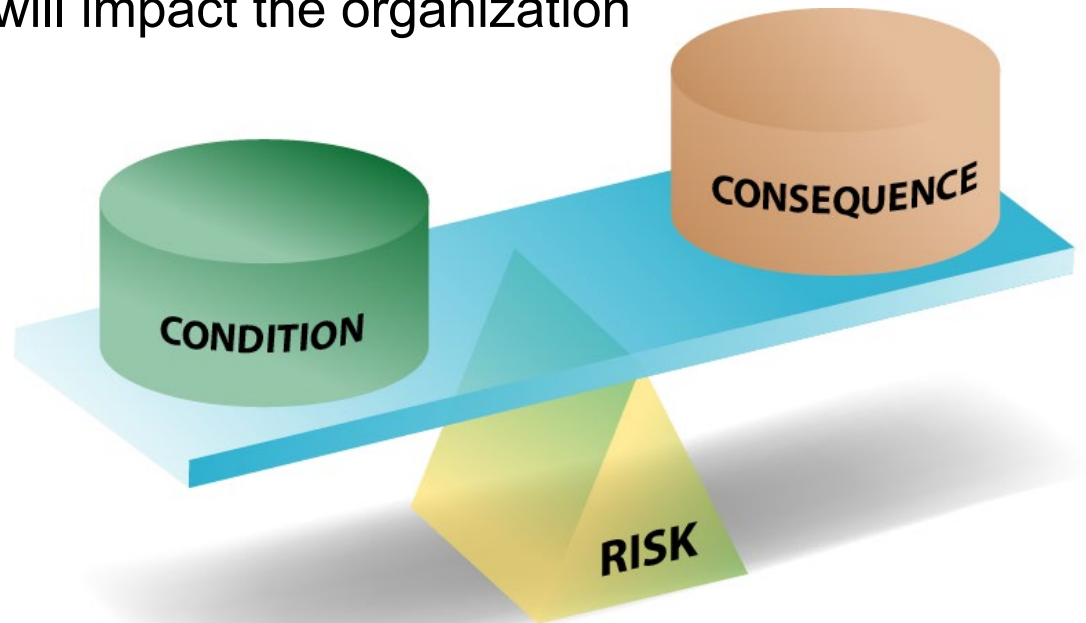
The focus of this class is OCTAVE-Allegro.

Fundamental Issues in an Information Security Risk Assessment

Coverage of the Risk Equation

Risk assessment must help the organization identify

- What could threaten the organization's operational resilience
 - Conditions
- What the likelihood is of the threat materializing
 - Uncertainty factor
- How the realized risk will impact the organization
 - Consequence



Focus on the Right Types of Risk

Operational risk must be the focus of the risk assessment.

- Failed internal processes
- Inadvertent or deliberate actions of people
- Problems with systems and technology
- External events

Move Past “Vulnerabilities”

Vulnerability assessment is NOT risk assessment.

Vulnerability assessment is for identifying “conditions.”

Conditions must be taken in the context of the organization’s unique operating circumstances.

There must be a consideration of “consequence” to be meaningful.

What Is OCTAVE?

A risk-based assessment

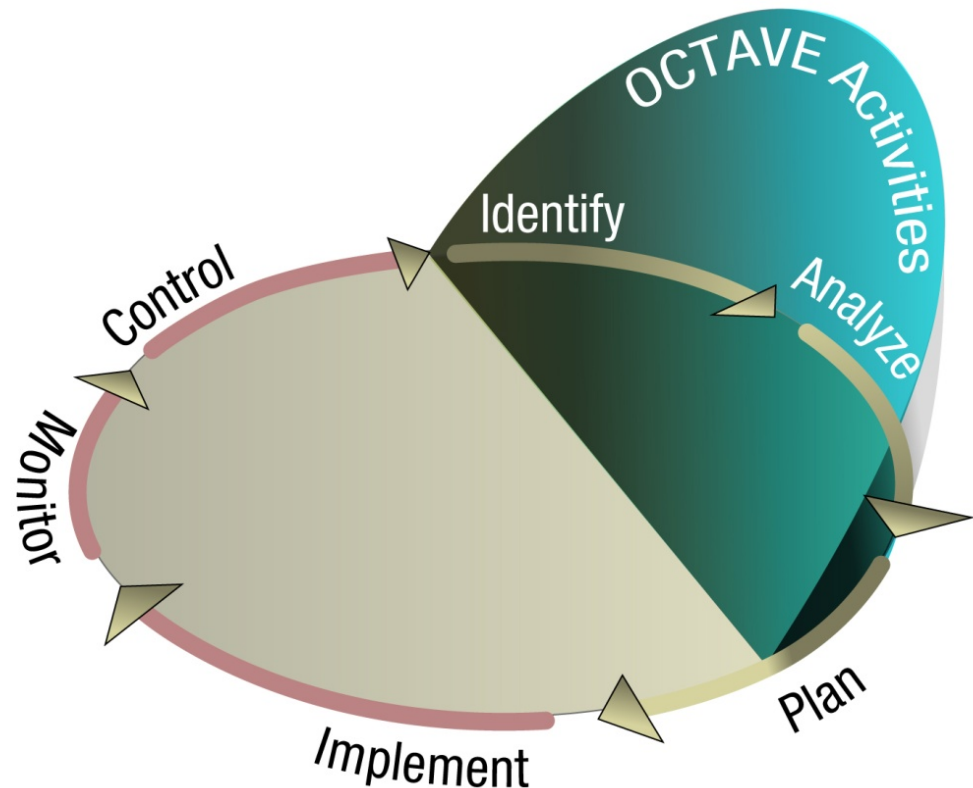
Leverage of people's knowledge of their organization's security-related practices to capture the current state of security practice within the organization

Focused on the asset level

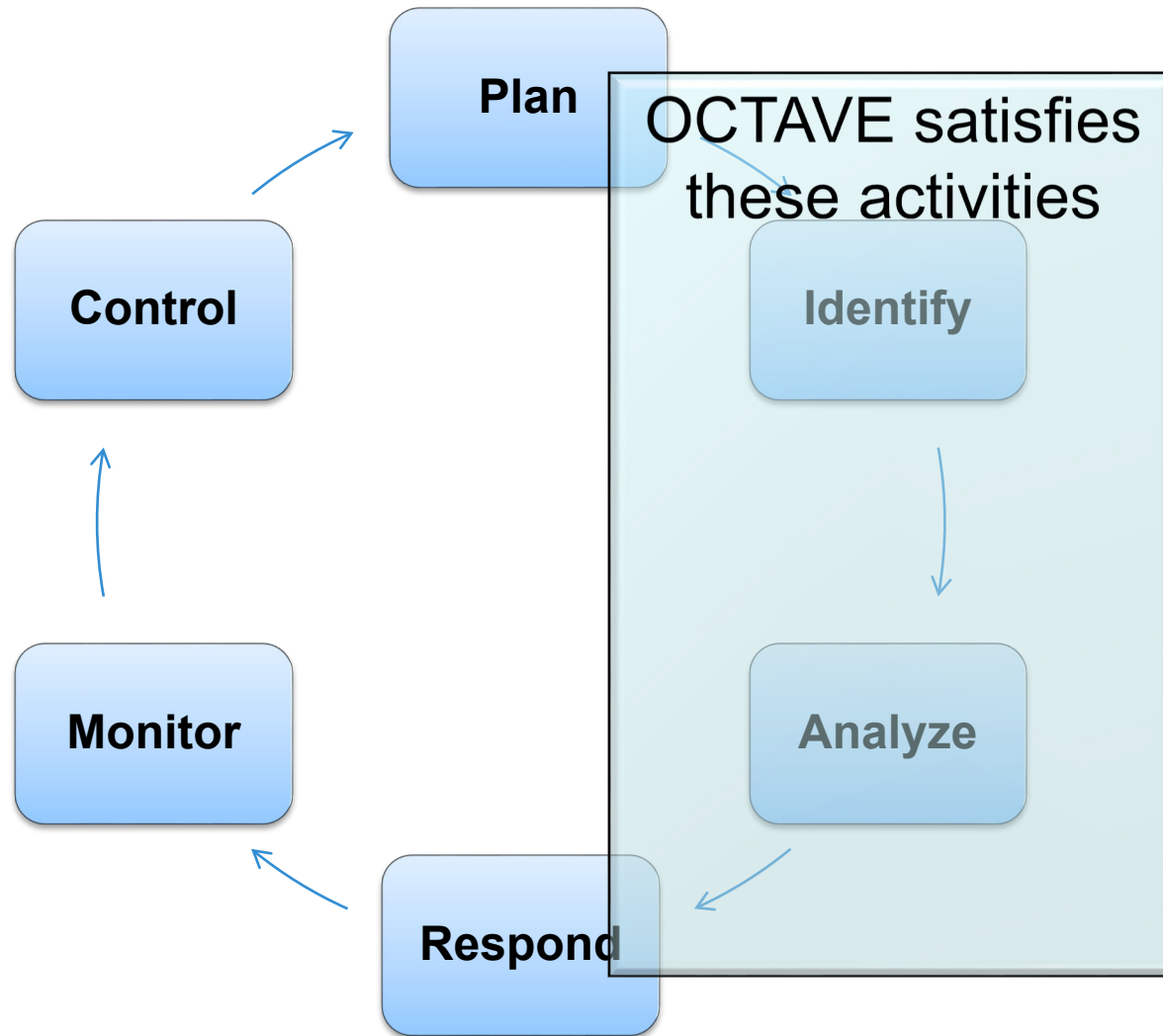
- People
- Information
- Technology
- Facilities

OCTAVE Approach

OCTAVE is at the center of a risk management approach to information security.



Continuous Risk Management process



OCTAVE Method

Originally developed for large-scale or complex organizations

A systematic, context-sensitive method for evaluating risks across the organization, involving

- Senior managers
- Operational area managers
- Staff

Defined by method implementation guide (procedures, guidance, worksheets, information catalogs) and training

OCTAVE-S

Defines a more structured method for evaluating risks in small or simple organizations

- Requires less security expertise in analysis team
- Requires analysis team to have a full, or nearly full, understanding of the organization and what is important
- Uses “fill-in-the-blank” as opposed to “essay” style

Defined by procedures, guidance, worksheets, information catalogs, and training

OCTAVE-Allegro

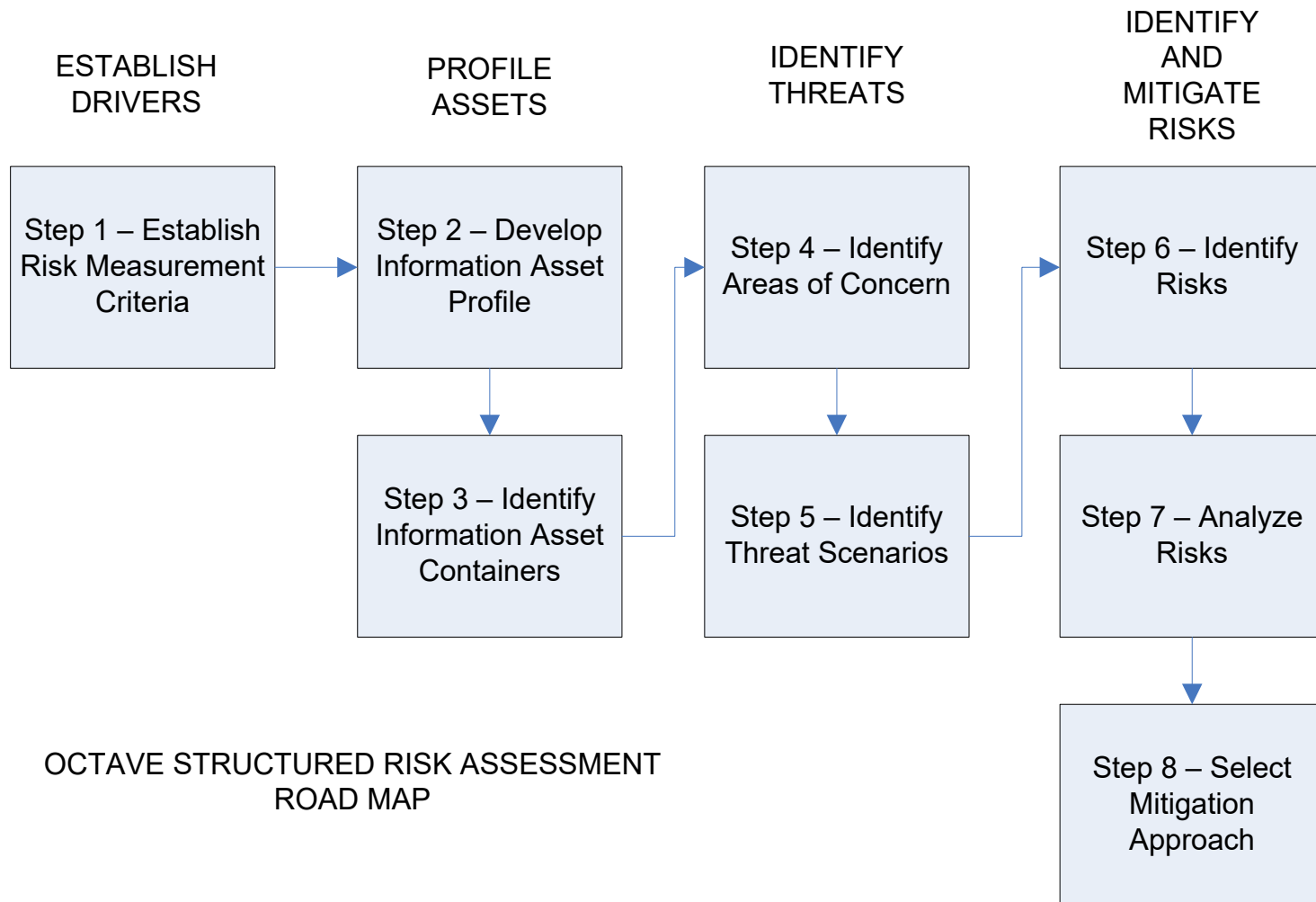
Derived from OCTAVE and OCTAVE-S

Defines a more structured method for evaluating risks by focusing on “information” assets

- Improves the ease-of-use, adoption, and repeatability
- Refines asset scope
- Reduces resource commitments
- Streamlines knowledge and training requirements

Performed in 8 steps

OCTAVE-Allegro Roadmap



OCTAVE STRUCTURED RISK ASSESSMENT
ROAD MAP

OCTAVE Analysis Team

An interdisciplinary team – consisting of

- Business or mission-related staff
- Information technology staff



Scoping the Evaluation

Scoping is the selection of the assets to include in the evaluation.

- Different areas of operation or business lines
- IT assets or systems
- The high-value services of the organization

Consider

- Primary areas crucial to mission or business objectives
- Major support functions
- Remote operations

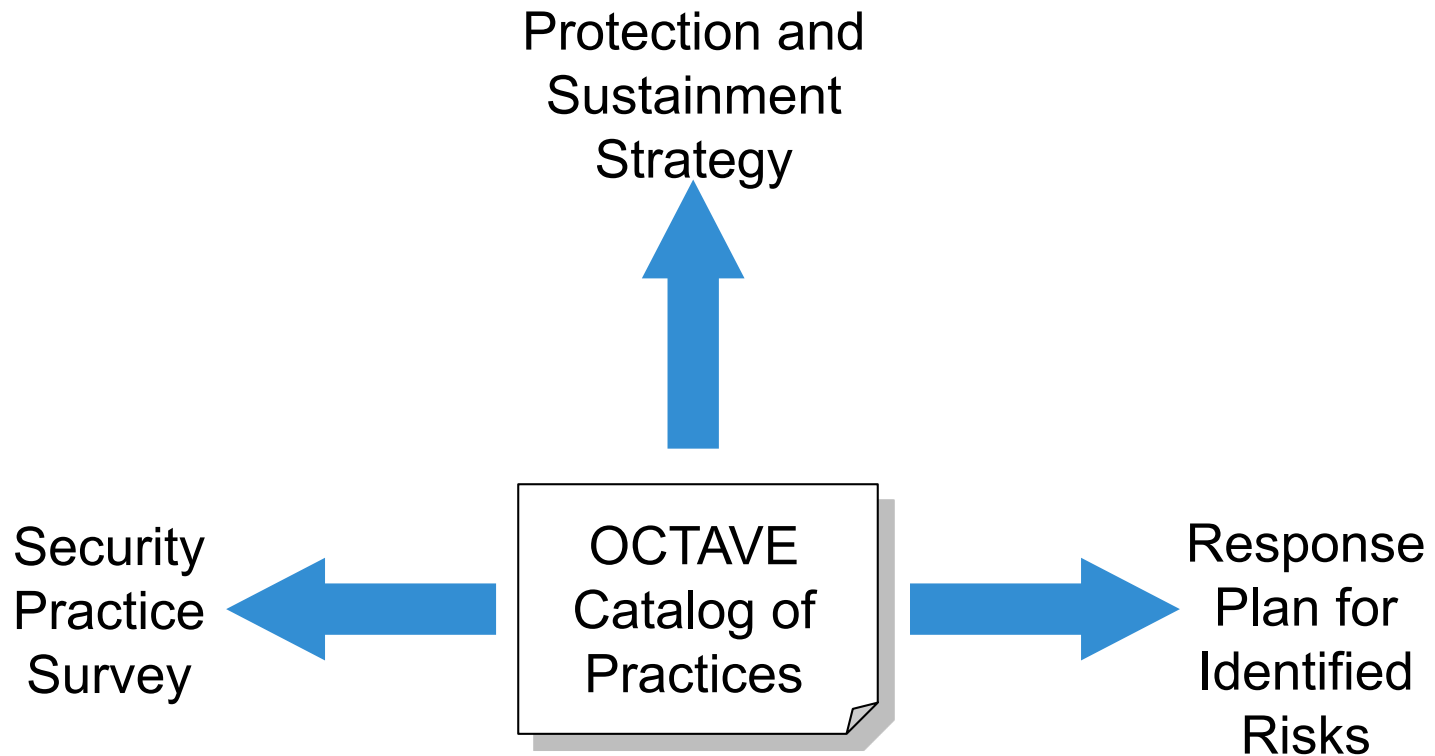
Note that you may need to focus on a smaller part of a large organization to get started.

Scoping the Allegro Evaluation

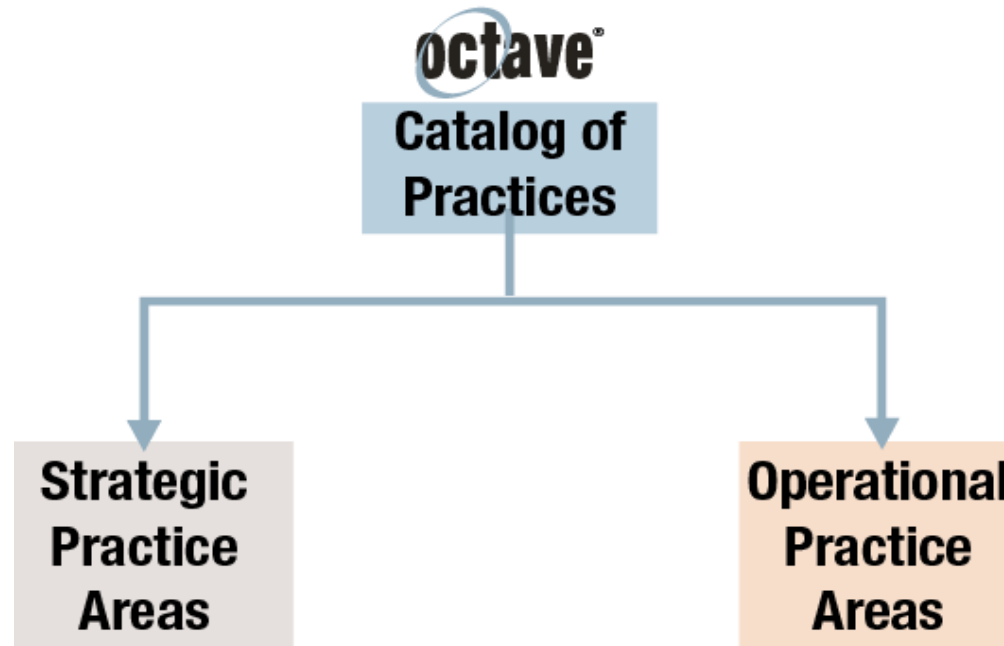
Scoping is the selection of information assets to include in the evaluation.

The purpose of assessing risks is to help the organization focus on those risks that have the most potential to prevent the organization from meeting its goals and objectives.

OCTAVE Catalog of Best Practices



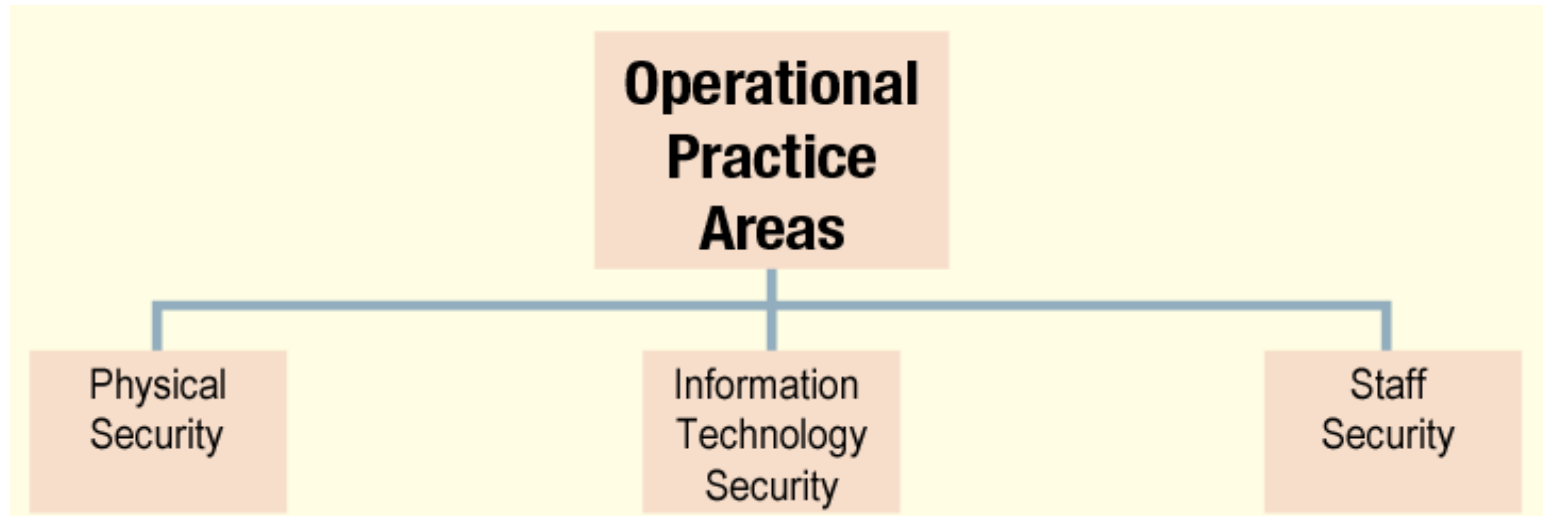
Basic Catalog Structure



Strategic Practice Areas



Operational Practice Areas



Physical Security Plans
and Procedures

Physical Access Control

Monitoring and Auditing
Physical Security

System and Network Management

System Administration Tools

Monitoring and Auditing IT Security

Authentication and Authorization

Vulnerability Management

Encryption

Security Architecture and Design

Incident Management

General Staff Practices

Outputs of OCTAVE

Protection Strategy



Helps define organizational protection and sustainment strategies

Response Plan



Plans designed to manage risk

Action List



Near-term action items

Outputs of the Allegro Process

Information asset profile for each critical asset assessed

Risk profile for information assets

- Relevant/contextual threat scenarios
- Prioritized risks
- Potential impacts
- Response strategies for high-priority risks

Risk Measurement Criteria

Organization-driven measurement benchmark

Aligned with an organization's risk tolerance and risk appetite

Used for assessing potential impact of risk on the organization's mission and business objectives

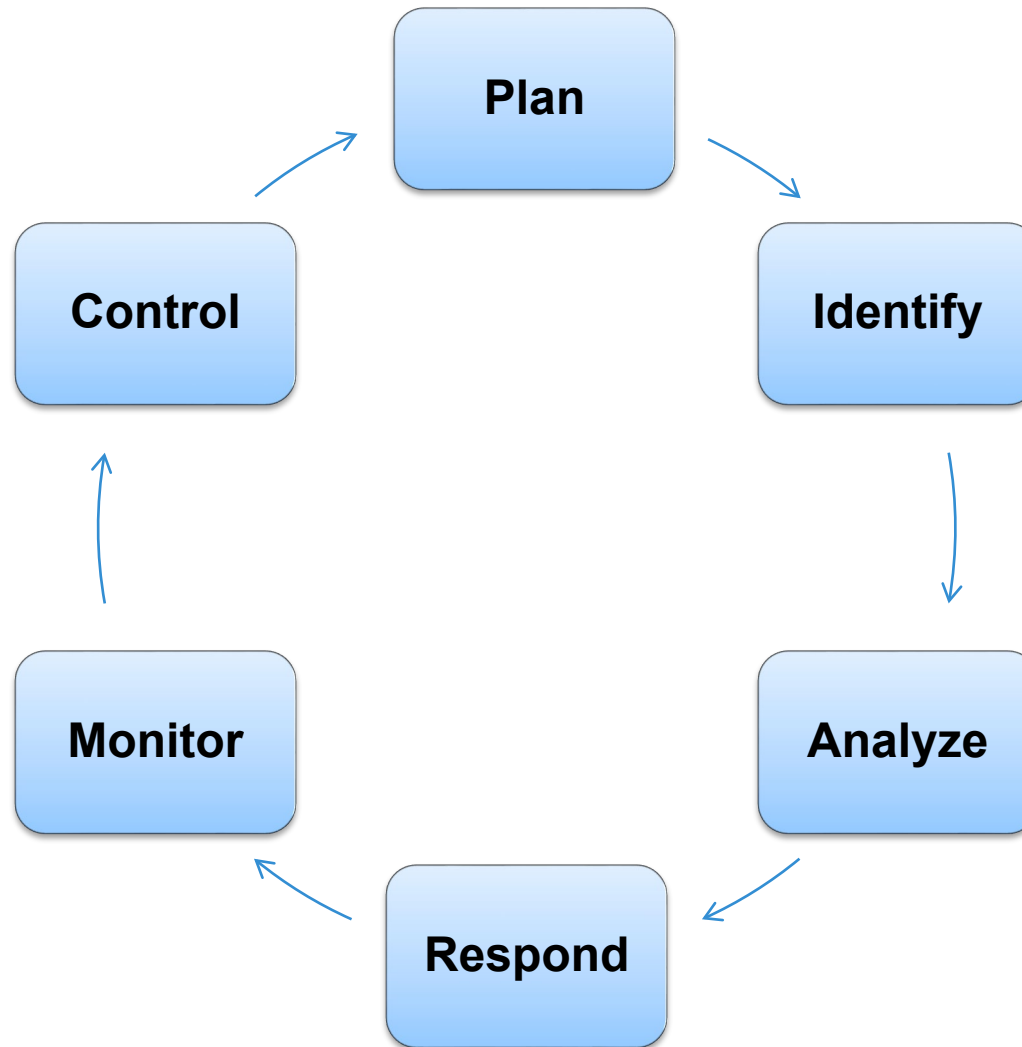
Gives risk meaning – what is the true impact to the organization?

Areas of Impact

Evaluation criteria should be considered for multiple types of impacts.

- Reputation
- Customer confidence
- Life/health/safety of customers and employees
- Fines/legal penalties
- Financial
- Productivity
- Other

Continuous Risk Management Process



Questions and Discussion



OCTAVE® Allegro Training

Step 1 – Establish Risk Measurement Criteria

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

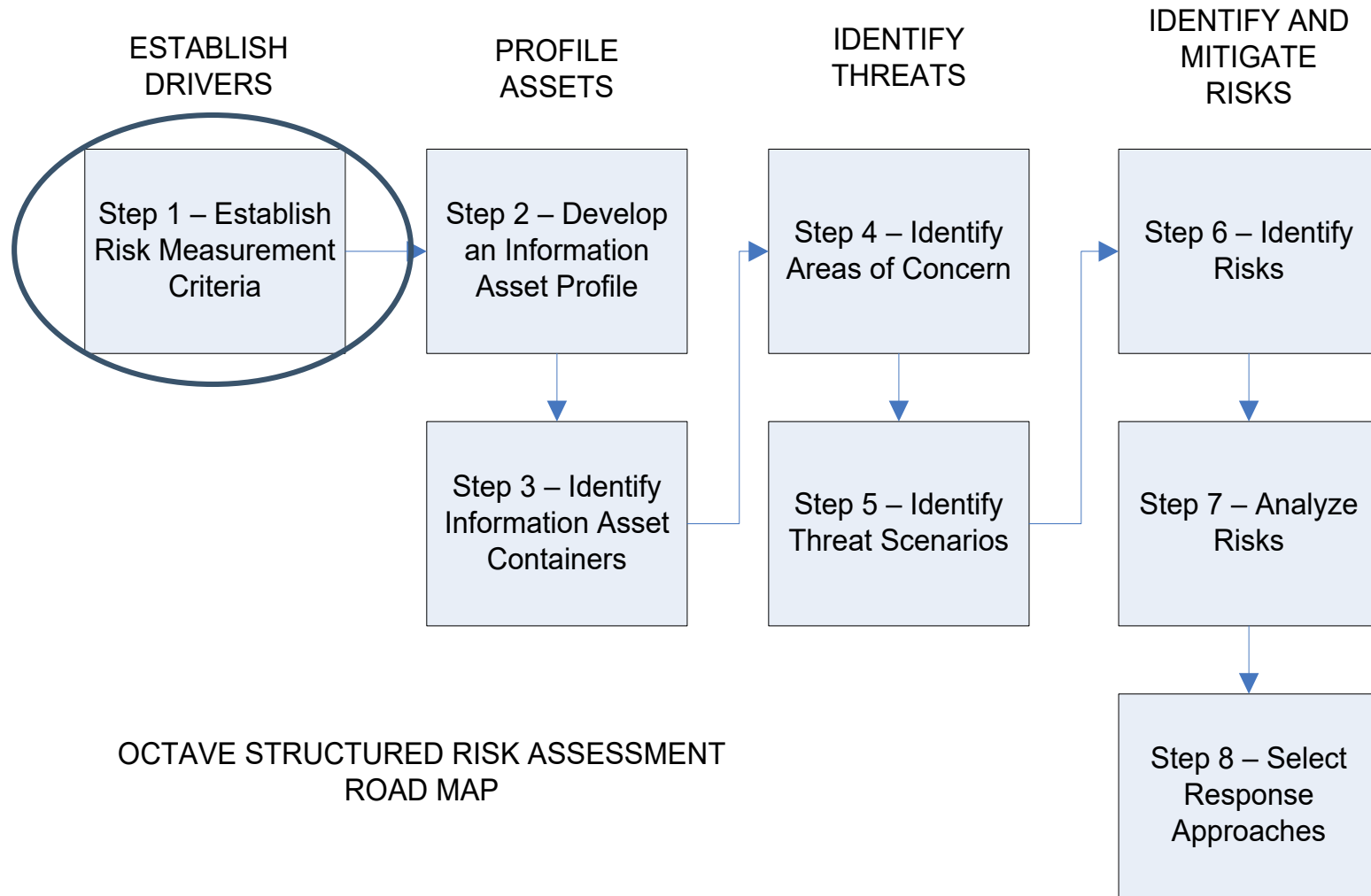
Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

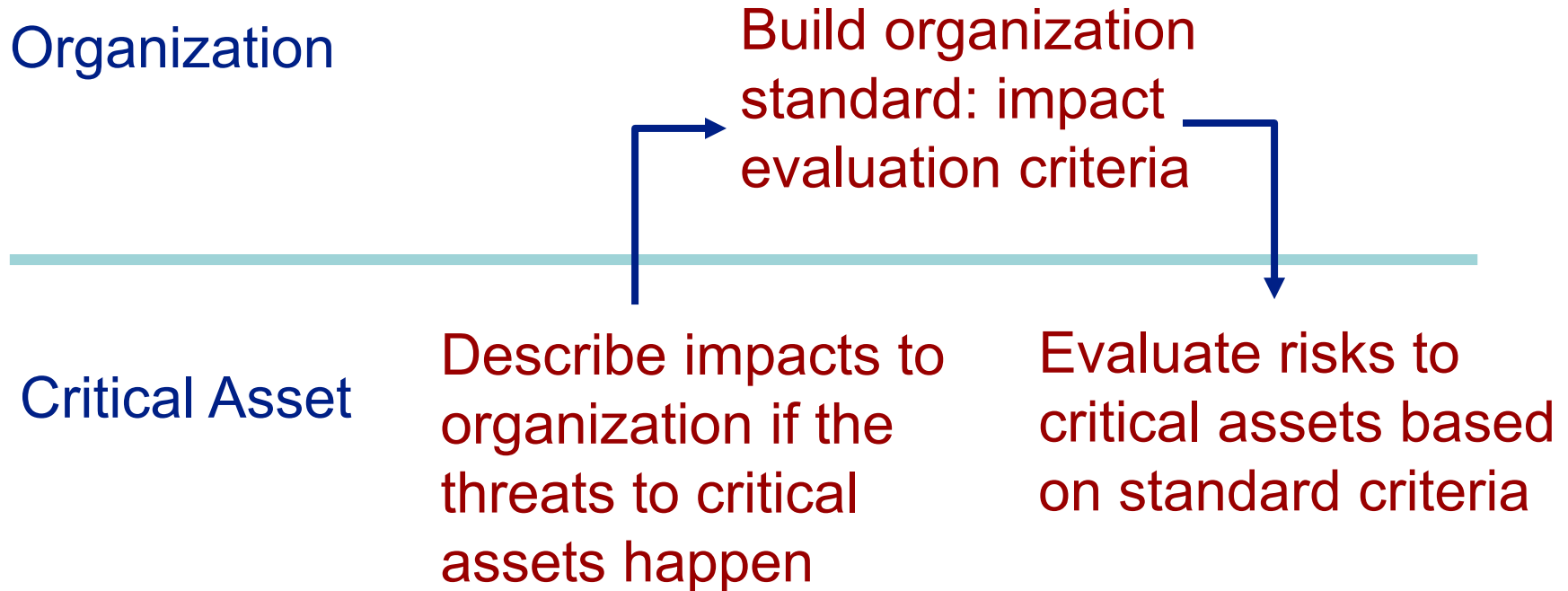
DM19-0487

OCTAVE Allegro Roadmap



OCTAVE STRUCTURED RISK ASSESSMENT
ROAD MAP

Asset and Organization Focus



Risk

Risk is a combination of the threat and the impact to the organization resulting from the following outcomes

- Disclosure
- Modification
- Destruction/loss
- Interruption

Risk Measurement Criteria -1

Organization-driven qualitative measurement benchmark

Used for assessing potential impact of risk on the organization's mission and business objectives

Can provide measurement of compliance with regulations

Provides way to prioritize risks for mitigation

Gives risk meaning – do you really care?

Risk Measurement Criteria -2



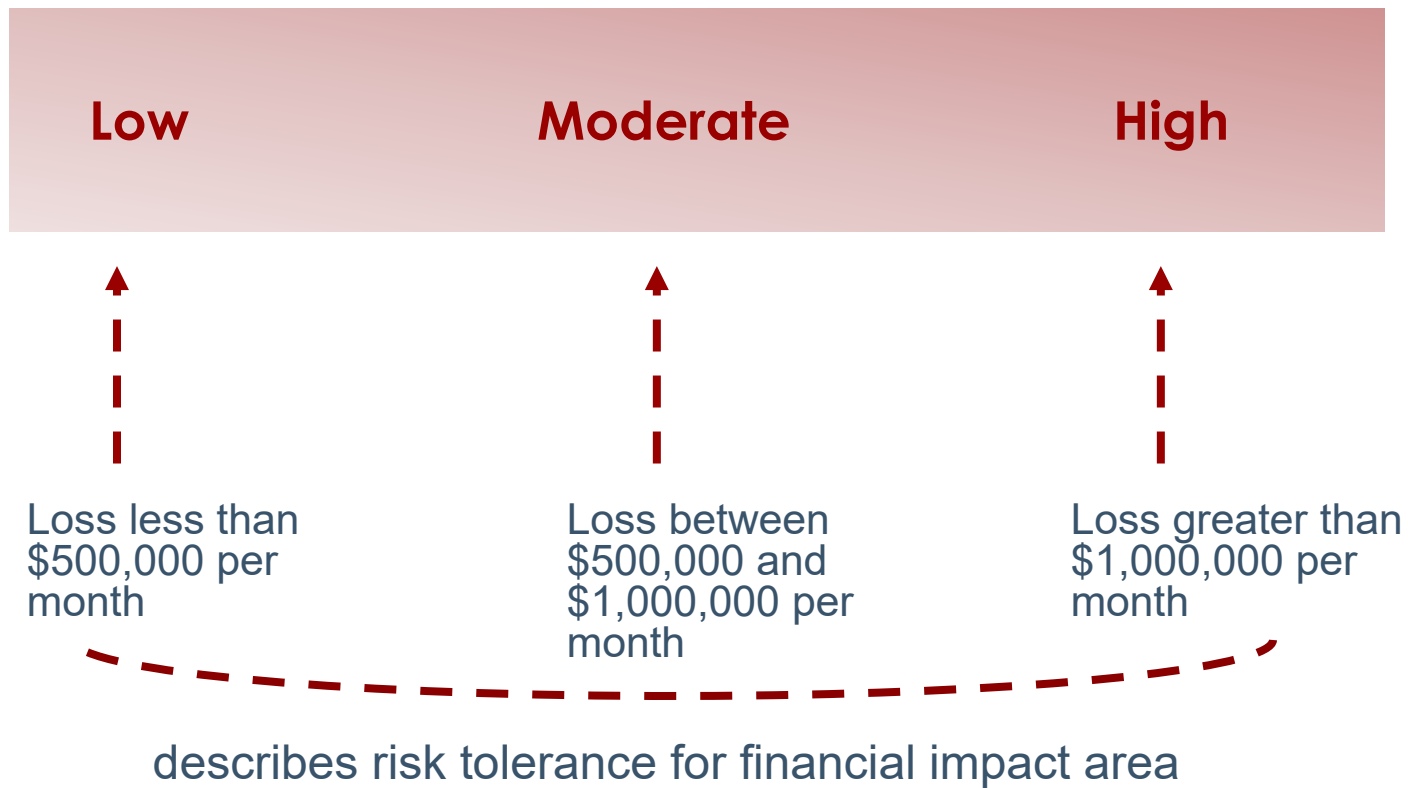
Risk Measurement Criteria -3

Places to look for risk measurement criteria in your organization

- Strategic or operational plans that outline the major business objectives of your organization
- Annual report if organization is public
- Legal requirements, regulations, or guidelines to which your organization must comply
- Results from other assessments (e.g., Business Impact Analysis (BIA) often conducted by Business Continuity or Disaster Recovery planners in your organization

Example of Impact Criteria

Impact area: Financial



Basis for Criteria

Many drivers can be used as the basis for risk measurement criteria.

- Areas of impact
- Security requirements of information assets

In Allegro, if you choose to develop your own criteria, you will use areas of impact as the basis.

Using Areas of Impact

Standard impact areas provided in Allegro

- Reputation/customer confidence
- Financial
- Productivity
- Life/health of customers
- Fines/legal penalties

Represent wide range of areas in which organization can be affected

Organization can add its own areas as well

Security Requirements

Security requirements can also form the basis for categorizing information and measuring risk impact.

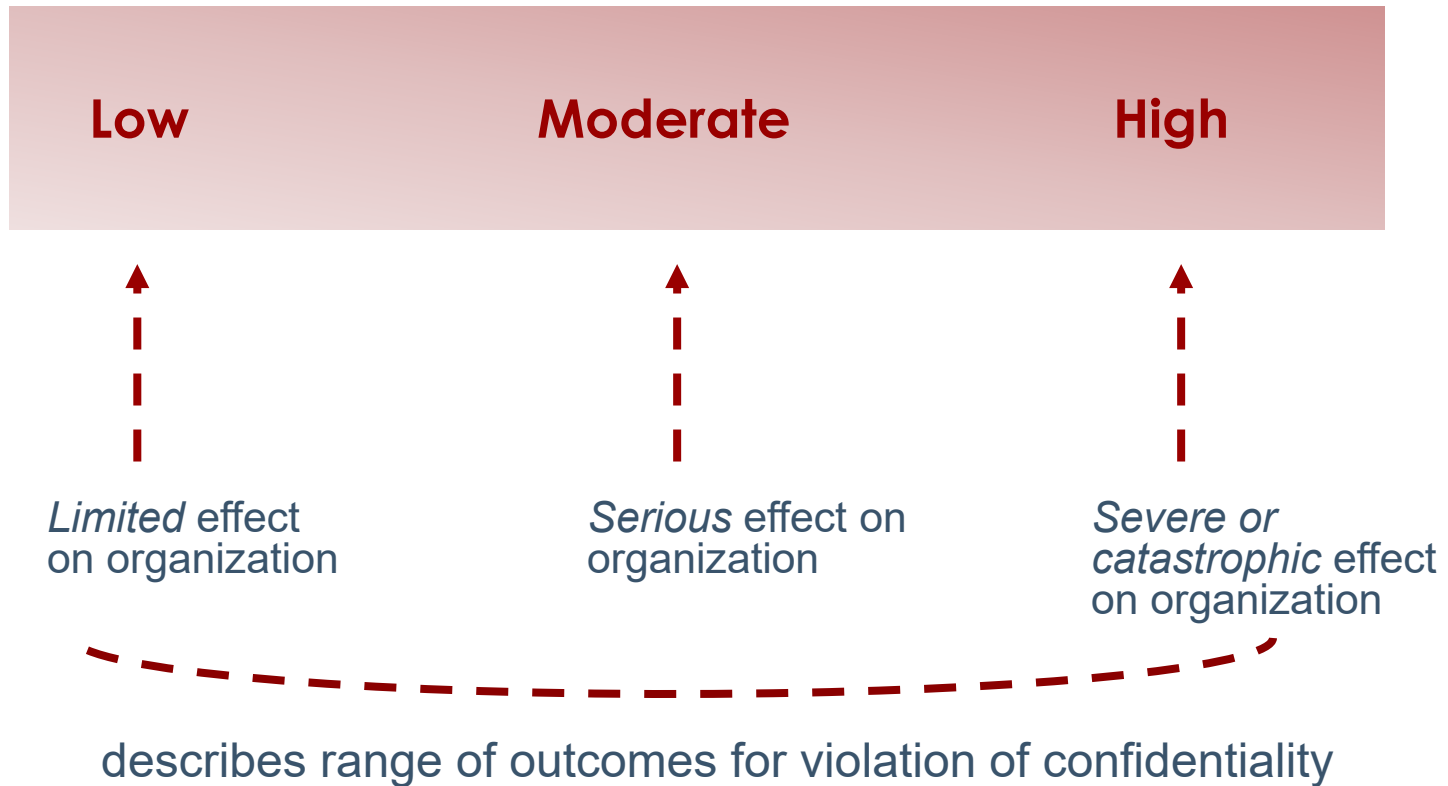
- Confidentiality
- Integrity
- Availability

Basic properties of all information assets

When violated, organization is impacted, but specific impact area not detailed.

Security Requirements Example

Result of violating confidentiality requirement



Which Basis to Use?

Depends on how much information is needed to categorize risks by their impact to your organization

Impact areas provide more precision and is the approach used in this assessment

Most important for organization-wide deployment – use consistent criteria across all risk assessments.

- If your organization already has requirements developed (e.g., FIPS199/200), use them.

Ranking Impact Areas -1

Not all impact areas are equal.

Example

- Consider an organization whose reputation with its customers is its differentiating factor in its industry. A high impact to its customer reputation would be of greater significance than perhaps an impact to its compliance with regulations.

Ranking Impact Areas -2

Creating a risk criteria provides a way to classify risks in terms of impact to the organization.

However, impacts in some areas may be more important to the organization than others.

Ranking impact areas adds additional contextual information for an organization to use when making choices about which risks to mitigate.

Same Outcome, Different Impact

For some risks, even though the outcome (e.g., disclosure) is the same, the impact to the organization may be different.

For example, a financial organization may find it more damaging to their customers' confidence if an *insider* deliberately exposes confidential information.

Background for Practice Exercises

The critical assets of the organization are known.

Some threats to the critical assets are known.

What risks are a concern to management is known.

Basic information security requirements are known.

Analysis team has knowledge of the organizational structure.

Book – *Managing Information Security Risks*

References

Identifying assets	pp. 89-93
Identifying security requirements	pp. 98-103
Risk evaluation criteria	pp. 176-177
Example risk evaluation criteria	pp. 341-343

Risk Measurement – Exercise 1

Develop a set of risk measurement criteria for the case study organization in each of the impact areas. Consider what constitutes high, medium, and low impacts for each area.

It may also be easier to start with the “high” criteria, and then define the “low” criteria. If you need an example, see the book, pp. 341-343.

Using the Widget Company case study
complete Step 1, Activity 1 on handout

Prioritizing Risks – Exercise 2

Rank the impact areas you created from most significant (5) to least significant (1).

Complete Step 1, Activity 2 on handout

Remember

There is one set of risk evaluation criteria for all assets; the criteria is not unique to the asset.

Evaluation criteria are created for areas of impact, which are related to the organization's key business objectives.

Step 1 Summary

Upon completion of Step 1, you have

- Developed risk measurement criteria
- Created a rank ordering for impact areas

Preview of Step 2

Coming in Step 2

- Selecting and profiling a critical information asset
 - What is an information asset?
 - Who owns it, who manages it?
 - How do we describe it?



OCTAVE[®] Allegro Training

Step 2 – Develop an Information Asset Profile

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

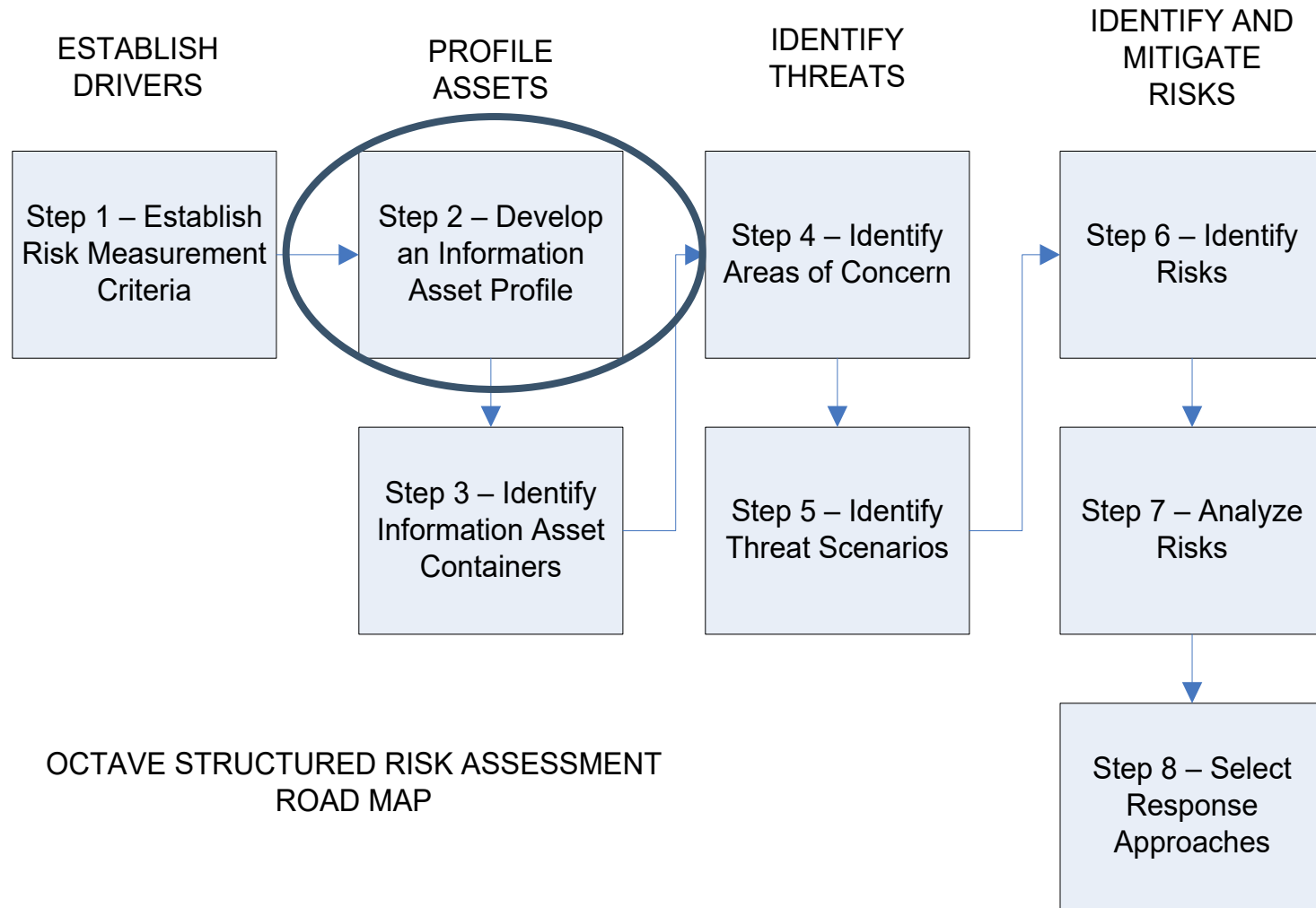
Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0487

OCTAVE Allegro Roadmap



OCTAVE STRUCTURED RISK ASSESSMENT
ROAD MAP

Objects of Risk Assessment

Services

Business processes

Assets

Services

The limited number of activities that the organization performs to deliver a service or to produce a product

Can be produced

- For internal use (i.e., administrative or support)
- For external use (i.e., producing widgets for customers)

Service mission must enable enterprise strategic objectives.

Business Processes

The activities that the organization (and its suppliers) perform to ensure that services meet their mission

Traverse the organization

Often are performed outside of the organization

Business process mission must enable service mission.

Assets

Something of value to the organization

People, information, technology, facilities

“Charged into production” of business processes and services

Value relates to the importance of the asset in meeting the business process and service mission

Assets must support business process and service missions.

What Is an Information Asset?

Information or data that is of value to the organization

Used by business processes to achieve goals

Can be physical “containers” (paper, CDs, thumb-drives) or electronic (files, databases)

Examples

- Patient records
- Intellectual property
- Customer information

High-value Information Assets

Information or data that is of value to the organization such that the organization would suffer a large, adverse impact if it is

- Disclosed to unauthorized people
- Modified without authorization
- Lost or destroyed
- Access is unavailable (interrupted)

What Is an Information Asset Profile?

A representation of an information asset describing its

- Unique features
- Qualities
- Characteristics
- Quantitative value (optional)

Attributes of Information Assets

Owners

Custodians

Containers

Security requirements

Information Asset Owners

Those individuals in the organization who

- Have responsibility for the viability, survivability, and resilience of the asset
- Set security requirements for the asset
- Ensure proper protection of the asset so that security requirements are met

Information Asset Custodians

Those individuals in the organization who

- Have responsibility to protect information assets that are stored, transported, or processed on containers owned or maintained by the custodians
- Accept responsibility for the asset from owner
- Ensure security requirements are implemented and achieved per owner's requirements

Information Asset “Containers”

Technology or physical assets where information assets are stored, transported, or processed

- Hardware
- Software
- Systems and applications
- Networks
- Paper
- PEOPLE

Information Asset Profile

Why is it important?

- Forms the basis for the identification of threats and risks in the upcoming steps
- Defines the Security requirements
- Ensures that assets are clearly and consistently defined
- Defines the asset boundaries
- Can be extended to included a quantitative value for the asset (optional)

Practice Exercise -1

Identify information assets

- Most important to your organization
- Used in day-to-day processes
- If lost, would significantly disrupt operations and goal achievement

Discuss and decide: What the critical assets of the widget company are and list them on the flipcharts.

Read Step 2, Activity 1

Practice Exercise -2

Which assets, if compromised, would have the biggest impact on the organization

- If the asset were **disclosed** to unauthorized people
- If the asset were **lost** or **destroyed**
- If the asset was **modified** without authorization
- If access to the asset was **interrupted**

Rank order the assets on your flipcharts in terms of importance (1 is most important)

Read Step 2, Activity 2

Practice Exercise -3

Document an information asset

- What is the asset called?
- Why is it important to the organization?
- How do you describe it?
- Who owns it?

Complete Step 2, Activities 3 – 6 using worksheet 8

Where We Are

We have determined our most critical asset(s).

Our rationale for selection is documented.

We have a description of the asset and the owner is identified.

So far, all of this work has been done by the analysis team.

Before moving to the next step, we will look at another way that is useful to gather information on assets.

Knowledge Elicitation Workshops -1

This is one way to gather the data.

Participants should be grouped by level, with no reporting relationships among the participants in any given workshop.

IT staff are usually interviewed in their own workshop.

It may also be advisable to include key customers or contractors/service providers in a workshop.

Knowledge Elicitation Workshops -2

To obtain the organizational perspectives on

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

The perspectives will come from

- Senior managers
- Operational area managers (including IT)
- Staff

Role of Analysis Team

Guide the activities and discussion of these workshops

Facilitate discussion

Check that the ideas are captured in context

Manage the project

- Keeps process on track
- Deals with difficult participants
- Keeps pulling for information
- Knows when to move on

OCTAVE Introduction Video

Small role play of the senior management workshop to demonstrate

- Facilitation and scribing
- Types of answers you are likely to get

Who's On The Videos

Scribe:
Quinn/IT

President Willis

Facilitator:
Coruna/sales

Plant Manager Ames

Vice-president Smart

table

OCTAVE

in the Widget Company

The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense
Copyright 2003 Carnegie Mellon University

OCTAVE

in the Widget Company

Introductions

Activity 1: Assets

Activity 2: Areas of Concern

Activity 3: Security Requirements

Activity 4: Practices Survey

Activity 5: Survey Discussion

Security Requirements -1

Confidentiality – Ensuring only authorized people (or systems) have access to an information asset.

Integrity – Ensuring that an information asset remains in the condition intended by the owner and for the purposes intended by the owner.

Availability – Ensuring that the information asset remains accessible to authorized users.

Remember: C. I. A.

Security Requirements -2

Outline the qualities of an asset that are important to protect.

- Confidentiality
- Integrity
- Availability

This should reflect what the requirements should be to protect the asset, not necessarily what is currently implemented.

OCTAVE

in the Widget Company

Introductions

Activity 1: Assets

Activity 2: Areas of Concern

Activity 3: Security Requirements

Activity 4: Practices Survey

Activity 5: Survey Discussion

Practice Exercise -4

Identify security requirements for the asset

- What is the confidentiality requirement?
- What is the integrity requirement?
- What is the availability requirement?
- Which requirement is most important?

Complete Step 2, Activities 7 & 8 using worksheet 8

Practices Survey (Optional)

To capture the “organizational view” of information security by

- Establishing what is important to the organization
- Determining how the organization currently addresses security
- Setting the scope of the evaluation by selecting critical assets
- Describing what is important about each critical asset
- Determining how critical assets are threatened

Protection Practices Survey

Provides direction for future information security efforts

Defines the strategies that an organization uses to

- Enable security
- Initiate security
- Implement security
- Maintain security

Current protection strategy is identified using surveys based on the catalog of practices.

The surveys are different to reflect the differences in the scope of work performed by staff, IT staff, and operational area managers.

Protection Practices Survey – Exercise 5

Use Handout Step 2 survey (condensed version) and answer as follows

- Yes – The practice is used by the organization.
- No – The practice is not used by the organization.
- Don't know – Respondents do not know if the practice is used by the organization or not.

Security issues are incorporated into the organization's business strategy.	Yes	No	Don't Know

OCTAVE

in the Widget Company

Introductions

Activity 1: Assots

Activity 2: Areas of Concern

Activity 3: Security Requirements

Activity 4: Practices Survey

Activity 5: Survey Discussion

Discussing Survey Results

Helps determine if the survey answers are accurate

Identifies any unusual concerns or details about security practices

Provides specific strengths (+) and weaknesses (-) that can be used later to enhance understanding of the survey information

OCTAVE

in the Widget Company

Introductions

Activity 1: Assets

Activity 2: Areas of Concern

Activity 3: Security Requirements

Activity 4: Practices Survey

Activity 5: Survey Discussion

Book – *Managing Information Security Risks*

References

Identifying assets	pp. 89-93
Identifying security requirements	pp. 98-103
Protection strategy survey	pp. 103-105
Protection strategy discussion	pp. 105-107
Completed survey example	pp. 345-361

Step 2 Summary

Upon completion of Step 2, you have created an information asset profile that

- Describes and bounds the information asset
- Documents the asset's owners
- Identifies the asset's security requirements
- Identified the actual security practices in place in the organization (optional)

Preview of Step 3

Coming in Step 3

- Identifying an information asset's containers
 - Where does the information asset live?
 - Where is it stored, transported, and processed?
 - Who are the custodians?



OCTAVE[®] Allegro Training

Step 3 – Identify Information Asset Containers

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

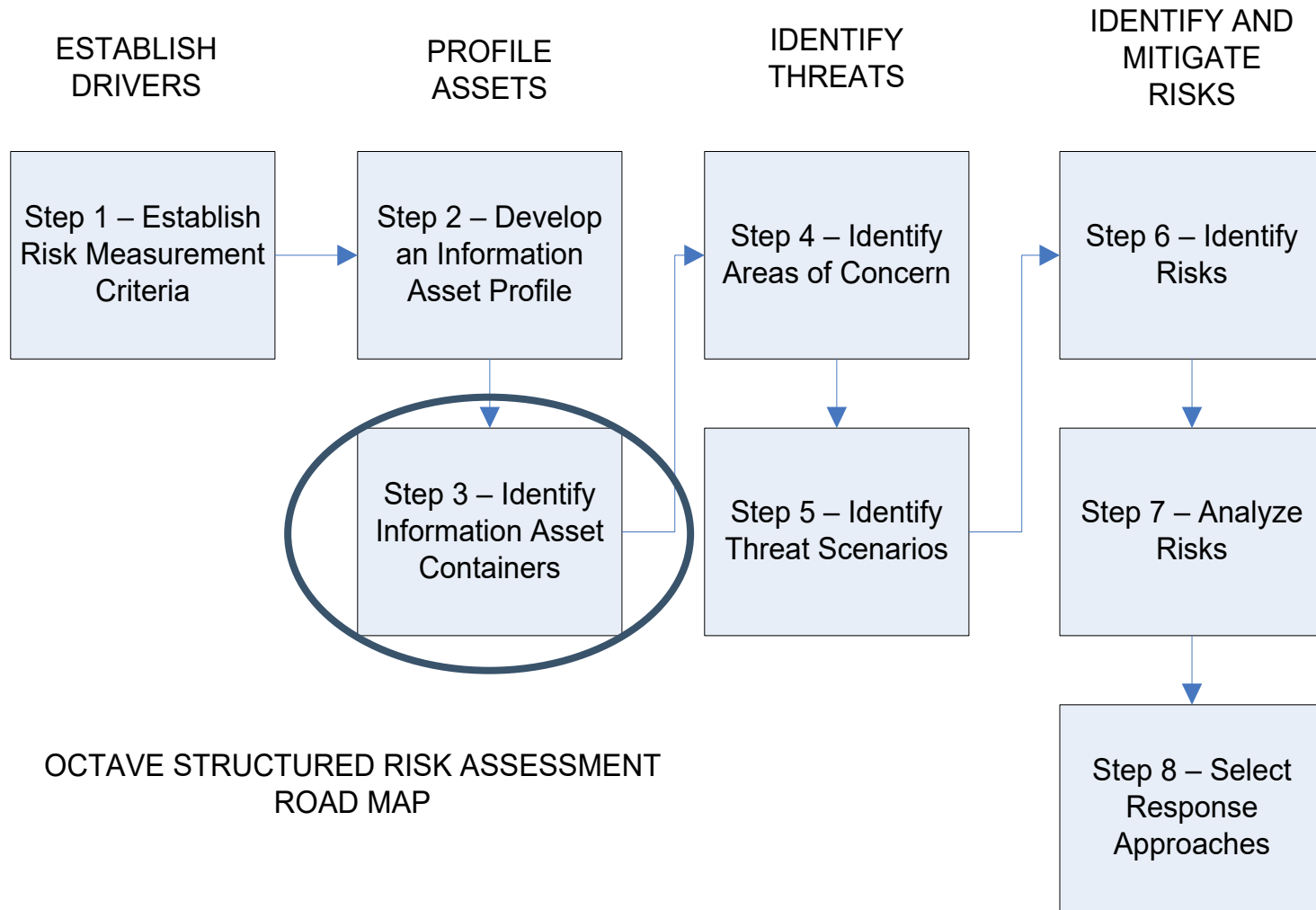
Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0487

OCTAVE Allegro Roadmap



OCTAVE STRUCTURED RISK ASSESSMENT
ROAD MAP

Risk Is Relative to a “Container”

Risk depends on where information assets are **stored, transmitted, or processed** and can be either internal or external to the organization.

Three types of containers

1. Technology
2. Physical
3. People

Information Asset “Containers” -1

Information assets often exist on containers that are not under the direct control of the organization that owns the information asset.

Example

- An organization that outsources its IT operations to a third party

Need to identify all of the locations where its information assets are stored, transmitted, or processed, whether or not they are within the organization’s direct control.

Information Asset “Containers” -2

The container concept is important to risk assessment because

- Threats to information assets are exploited via vulnerabilities at the container level
- Securing the container protects the information asset

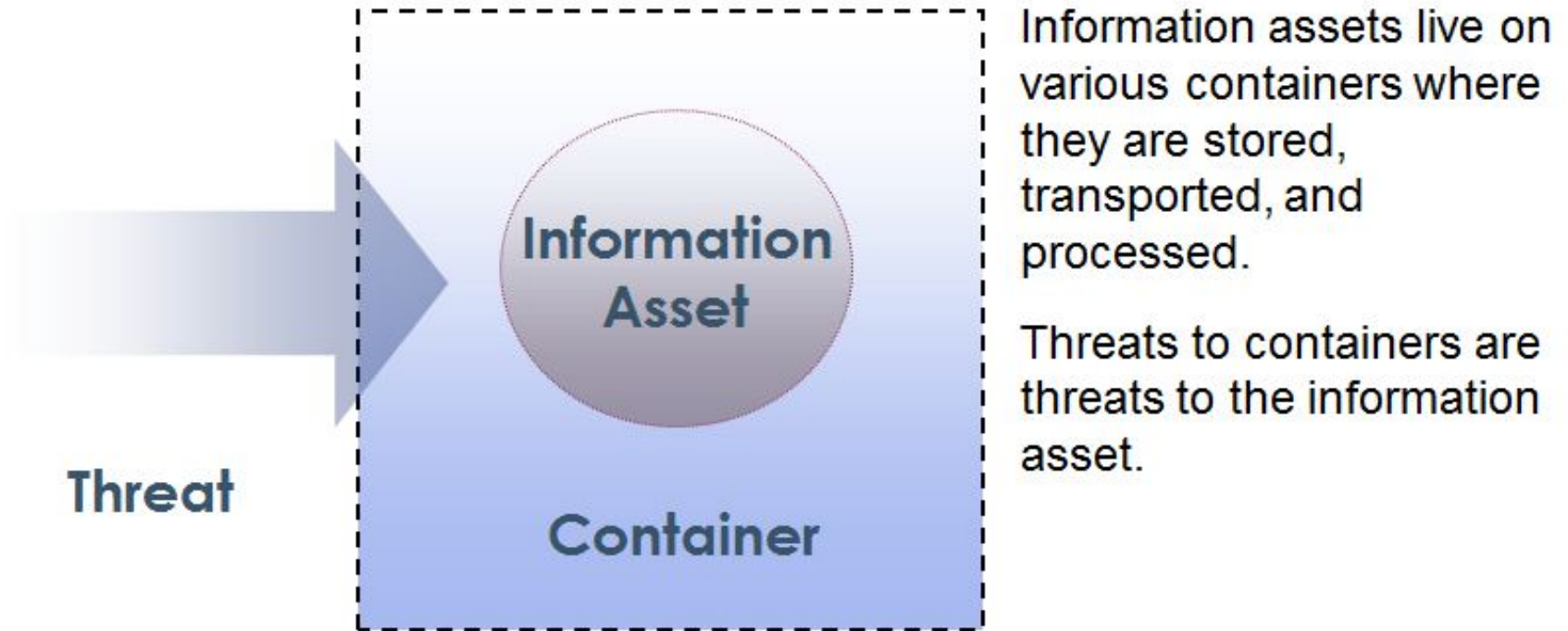
Information Asset “Containers” -3

Risk to an information asset can only be considered in the context of the asset's containers.

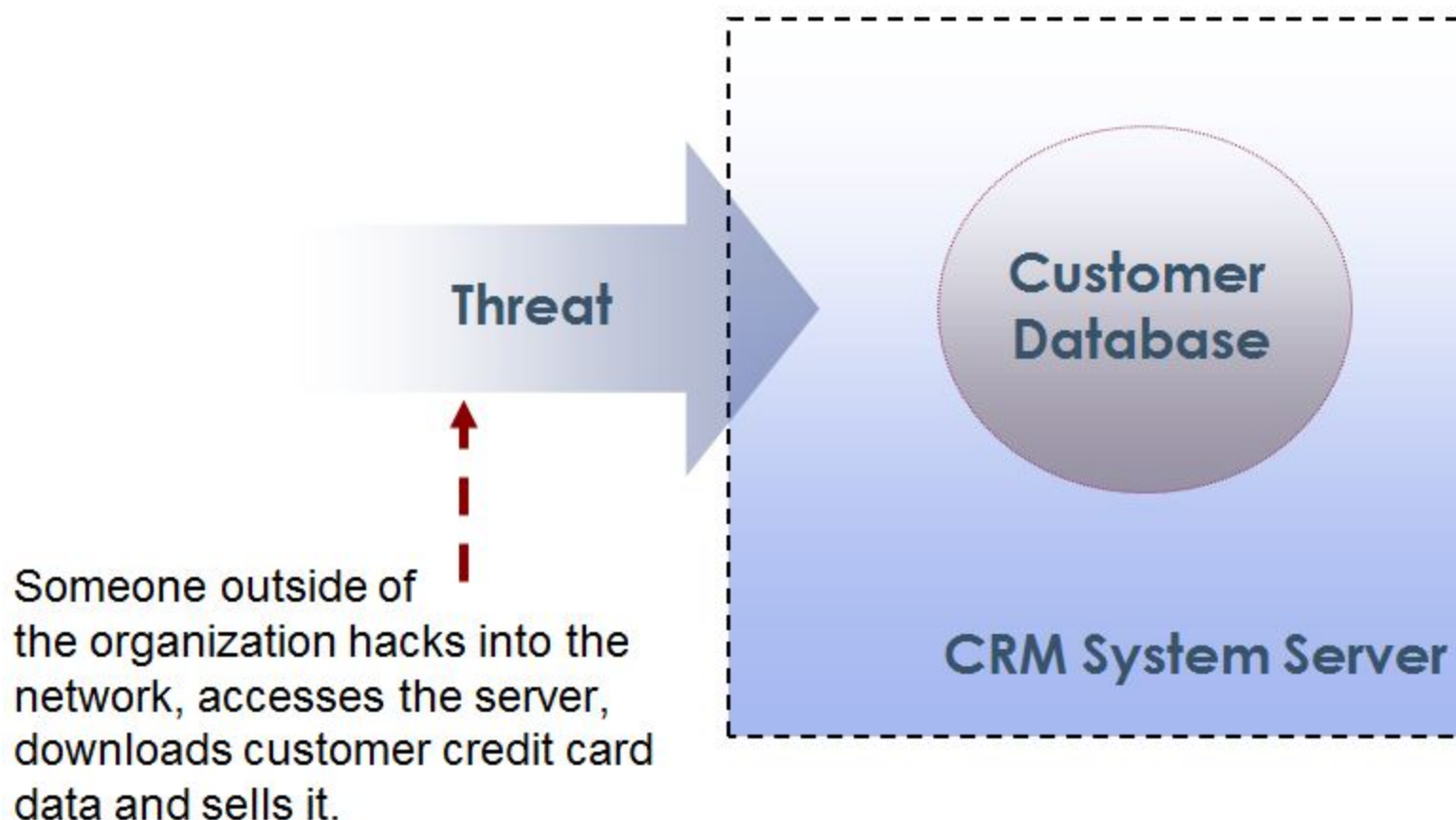
Protection of an information asset can only be considered with respect to controls at the container level.

Security requirements for the asset are satisfied at the container level.

Information Asset “Containers” -4



Information Asset “Containers” -5



Technology Containers -1

Information assets are **stored, transmitted, and processed** by technical containers such as

- Hardware
- Software
- Networks
- Systems
- Applications

Technology Containers -2

Technical containers provide a direct route to the information asset.

Threats that allow unauthorized users to electronically or physically access technical containers also provide access to the information asset.

Physical Containers

Information assets may be stored or transmitted on paper, in physical file rooms or other places.

Information assets are transmitted as these paper files are copied, mailed, passed around.

Threats that allow unauthorized users to physically access paper or file folders also provide access to your information asset.

People Containers

People may also be a means for **storing** or **transporting** information assets.

People may “know” or communicate information that is valuable to the organization.

People may also be the only source of some information, such as intellectual property.

Threats that allow information that people know to be inaccessible or permanently lost or destroyed threatens the information asset.

Special Considerations

A container may contain more than one information asset.

These information assets could have conflicting security requirements.

Custodians are challenged in this situation because they must satisfy both sets of requirements.

Practice Exercise

Identify key information asset containers

- What system or applications use the asset?
- On what hardware might it be found?
- What people know this asset?
- Are there other places where it exists?

**Complete Step 3, Activity 1 using
worksheets 9a, 9b, 9c**

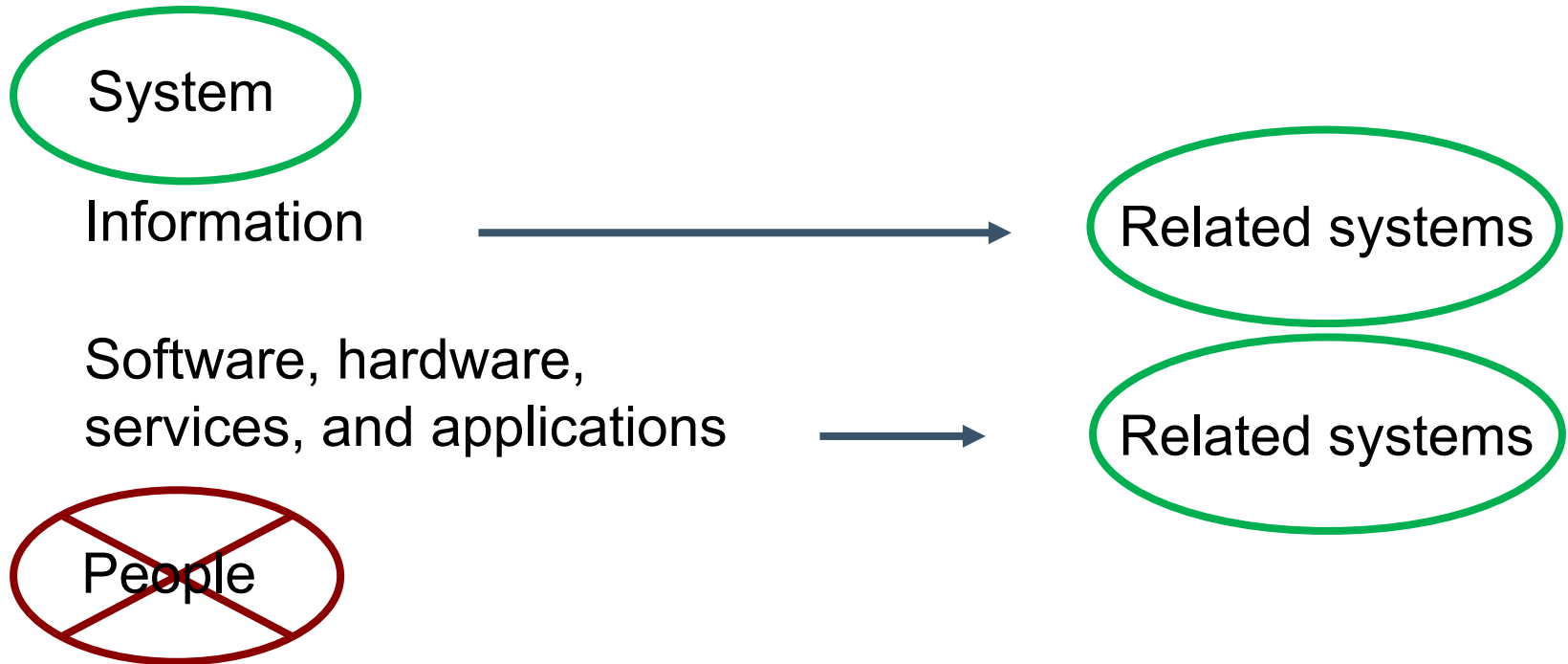
If You Decide to Include a Technical Vulnerability Evaluation in Step 3 -1

1. Identify the containers – where a critical asset “lives” on the network.
2. Identify access paths to the asset – potential exploit routes using the network.
3. Select representative classes of components and specific devices and strategies for evaluating those components.
4. Use vulnerability tools to perform a targeted vulnerability evaluation on the selected devices.

If You Decide to Include a Technical Vulnerability Evaluation in Step 3 -2

5. Generate vulnerability summary, specifying the potential impacts to critical assets.
6. Analyze results for threats to the critical assets and update threat profiles.
7. Review IT security practices.
8. Identify immediate action items to address major infrastructure weaknesses and recommendations for consideration during mitigation strategy.

Containers to be Considered



Selecting the Right Strategy for Step 3

Does the IT staff have experience conducting vulnerability evaluations?

Is this something that is done on a regular basis?

- If so, request the most current copy of the results.

Are external resources available to assist?

Do you have a good, current network map?

Is the Infrastructure Vulnerable?

Technology vulnerability

- Features in a system that can allow unauthorized action

Exploit

- Process of using a technology vulnerability to violate security policy

Every infrastructure has vulnerabilities.

- Design vulnerabilities
- Implementation vulnerabilities
- Configuration vulnerabilities

Vulnerability Evaluation Tools

Vulnerability tools identify

- Known weaknesses in technology (e.g., unapplied patches)
- Improper configurations of 'well known' administrative functions, such as
 - File permissions on certain files
 - Accounts with null passwords
- Information an attacker can determine about your systems and networks

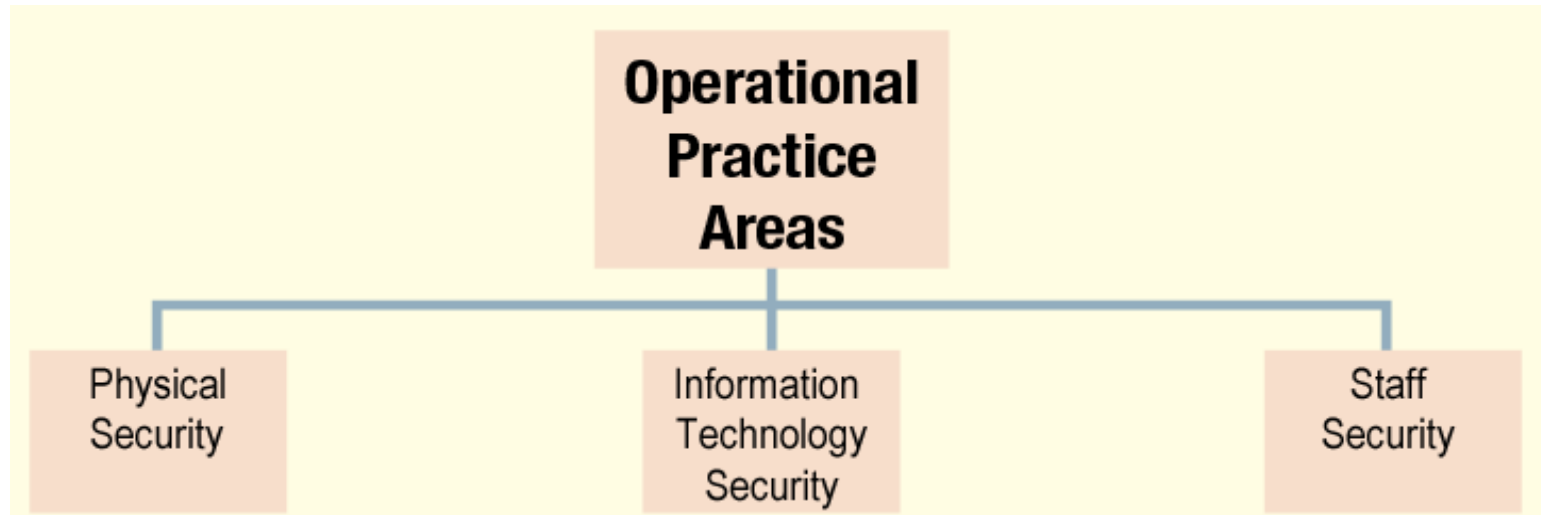
What Vulnerability Evaluation Tools Do Not Identify

Misapplied or improper system administration (users, accounts, configuration settings)

Unknown vulnerabilities in operating systems, services, applications, and infrastructure

Incorrect adoption or implementation of organizational procedures by IT personnel or users

Practices Usually Included in Vulnerability Assessment



Physical Security Plans and Procedures

Physical Access Control

Monitoring and Auditing Physical Security

System and Network Management

System Administration Tools

Monitoring and Auditing IT Security

Authentication and Authorization

Vulnerability Management

Encryption

Security Architecture and Design

Incident Management

General Staff Practices

System of Interest

Where the critical asset “lives” on the network

The system that is most closely linked to the critical asset gives

- Legitimate users access to a critical asset
- A threat actor access to a critical asset

If the critical asset *is* a system, then it is its own system of interest.

It is possible to have multiple systems of interest for a critical asset.

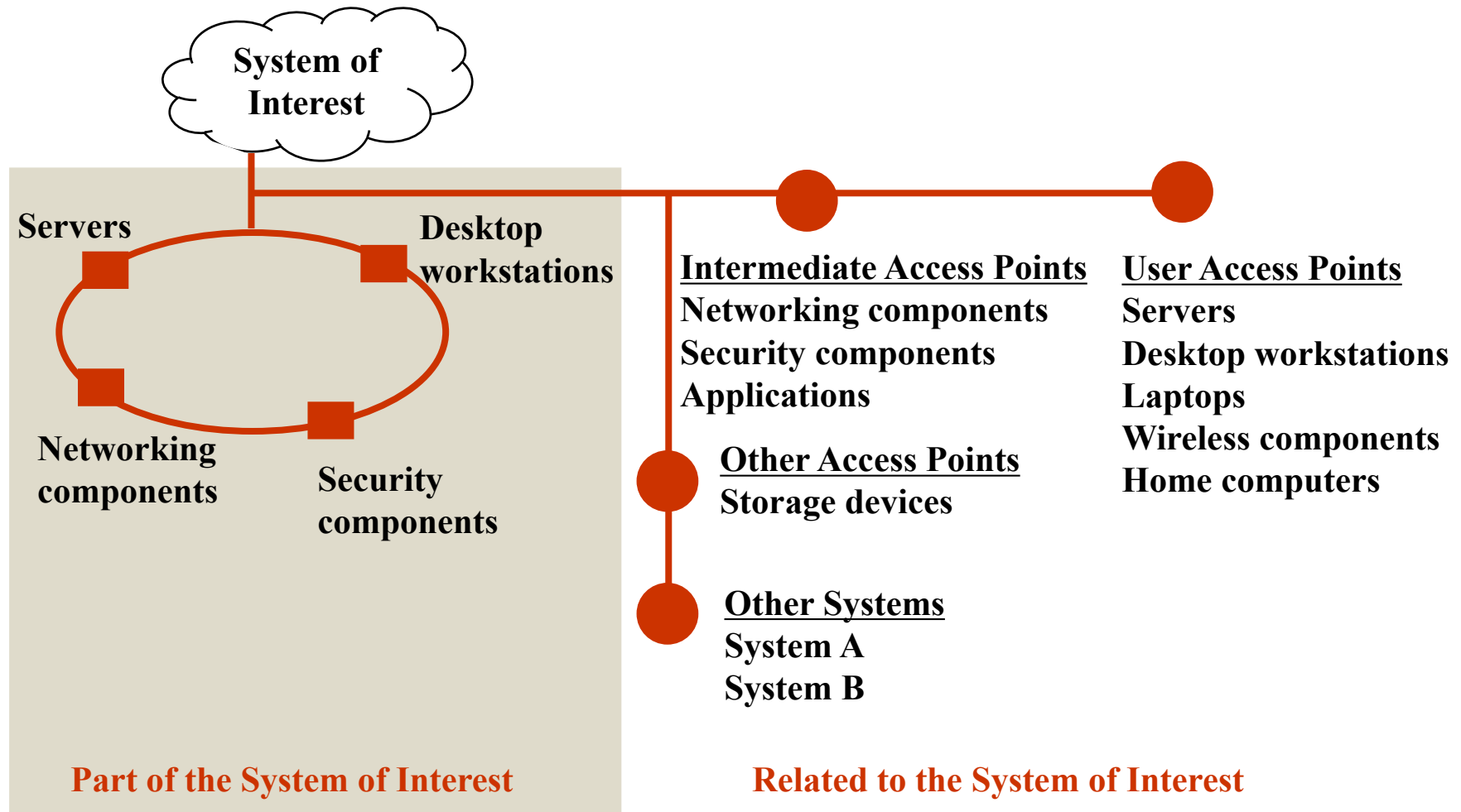
Accessing Assets

Access paths are the ways in which each system of interest can be accessed via your organization's network(s).

Access points are the types of components used to access a system of interest, including

- User access points
- Intermediate access points
- Other access points
- Other systems

Potential Access Paths



Select Key Classes of Components

Types of devices and components that are related to the system of interest and access paths such as

- Servers
- Networking components
- Security components
- Workstations
- Home computers
- Laptops
- Storage devices
- Wireless components
- Other

Select Types of Vulnerability Evaluation Tools

Operating system scanners

Network infrastructure scanners

Specialty, targeted, and hybrid scanners

Checklists

Scripts

Approval for Automated Tools

Automated tools can affect the operations of the organization.
You must

- Determine what effects the tools will have on the organization's operations and personnel
- Gain approval to run the tools and agreement on when they can be run
- Notify all personnel who may be affected

You may also be required to estimate costs for management approval.

Physical Security Options

Your strategy may include expanding OCTAVE to include a physical security audit or evaluation.

The same process can be used for planning a physical security evaluation for assets with physical access or other types of physical threats (e.g., natural disasters/sabotage).

- Define a strategy
- Identify key components of the physical infrastructure (e.g., specific rooms, doors, filing cabinets, etc.)
- Define a method or tool for evaluating the components
- Carry out the evaluations

Widget Company Results – Class Discussion Exercise

Review the results from Step 3 of the Widget Design case study.

Refer to the Widget Company background information.

Discussion

- What do you think about their choices?
- Did they leave anything out?

Book – *Managing Information Security Risks*

References

Identifying key classes of components pp. 143-150

Selecting components pp. 150-154

Step 3 Summary

Upon completion of Step 3, you have identified the key containers on which the information asset lives.

- Helps to identify vulnerabilities and threats in real-world context
- Provides insight into the types of controls necessary to protect the asset

Preview of Step 4

Coming in Step 4

- Identifying real-world conditions or situations that could affect your information asset
 - Consider the container(s) that could be threatened
 - Consider internal and external threats



OCTAVE[®] Allegro Training

Step 4 – Identify Areas of Concern

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

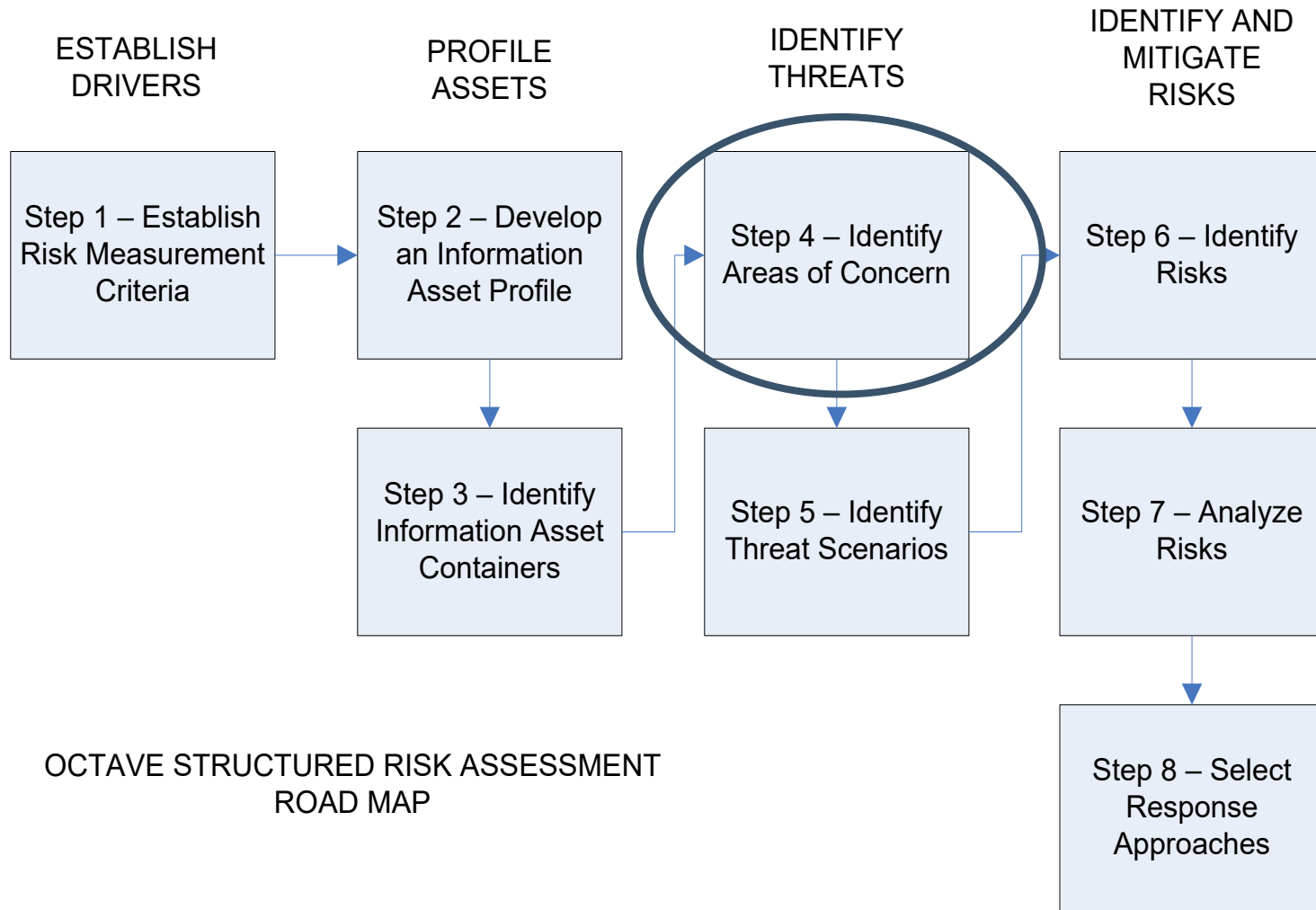
Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0487

OCTAVE Allegro Roadmap



OCTAVE STRUCTURED RISK ASSESSMENT
ROAD MAP

What Is an Area of Concern?

An area of concern is a real-world condition of situation that could affect an information asset in your organization.

Examples

- *Patient case information is stored in the trunk of my car when I make home visits.*
- *My laptop contains lots of sensitive customer information but I do not think the data is encrypted.*

Areas of concern describe possible threats against information assets.

Areas of Concern

Situations where you are concerned about a **threat** to your important information assets

Typically, areas of concern have a **source** and an **outcome** – a causal action that has an effect on the organization.

Example Areas of Concern

An employee accidentally accesses the medical records of a patient and discloses their contents.

An outsider deliberately accesses various patient medical records and makes unauthorized modifications to them.

Frequent system crashes result in an unauthorized modification of medical records.

Paper medical records are lost or destroyed due to a flood.

OCTAVE

in the Widget Company

Introductions

Activity 1: Assots

Activity 2: Areas of Concern

Activity 3: Security Requirements

Activity 4: Practices Survey

Activity 5: Survey Discussion

Areas of Concern – Exercise 1

In your teams, discuss scenarios that threaten your important information assets. Consider sources and outcomes. Use the AOC (spider diagram) for ideas.

Record the areas of concern on the flipchart.

Try to capture both the source and outcome as well as some idea of the impact to the organization.

What Is a Threat?

A threat is an indication of a potential undesirable event.

- A situation or scenario involving a person or natural occurrence
- Resulting in an undesirable outcome

Threat Is a Part of Risk -1

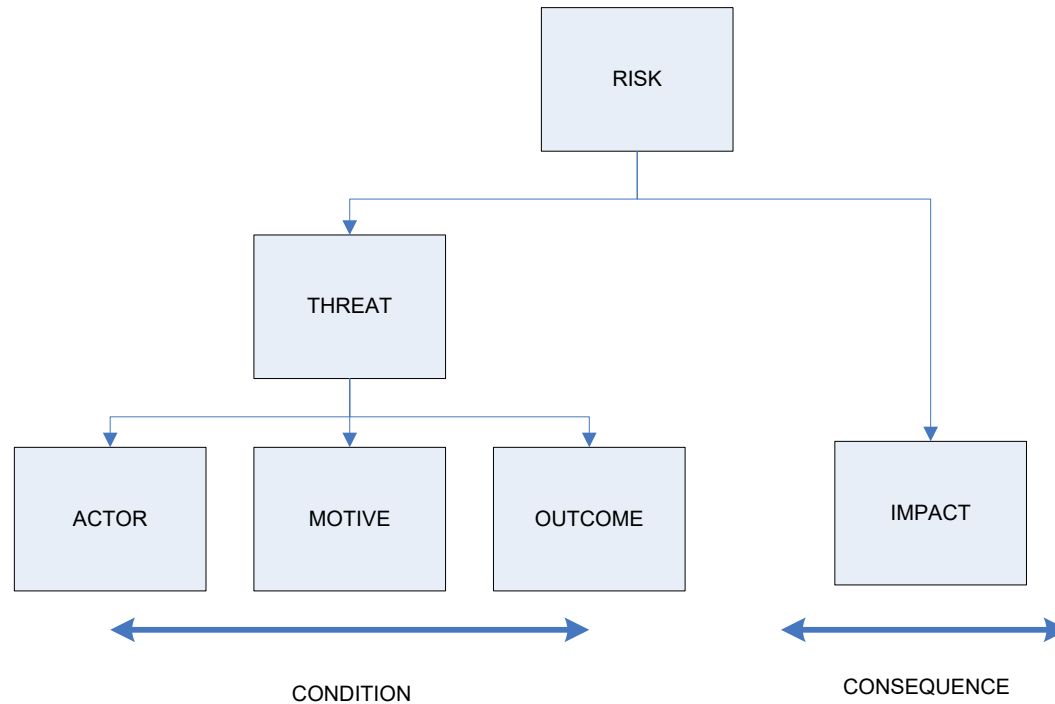
A threat must possess the means, motive, and opportunity to exploit a weakness or vulnerability on a container that stores, transports, or processes an information asset.

The threat can be a circumstance or event.

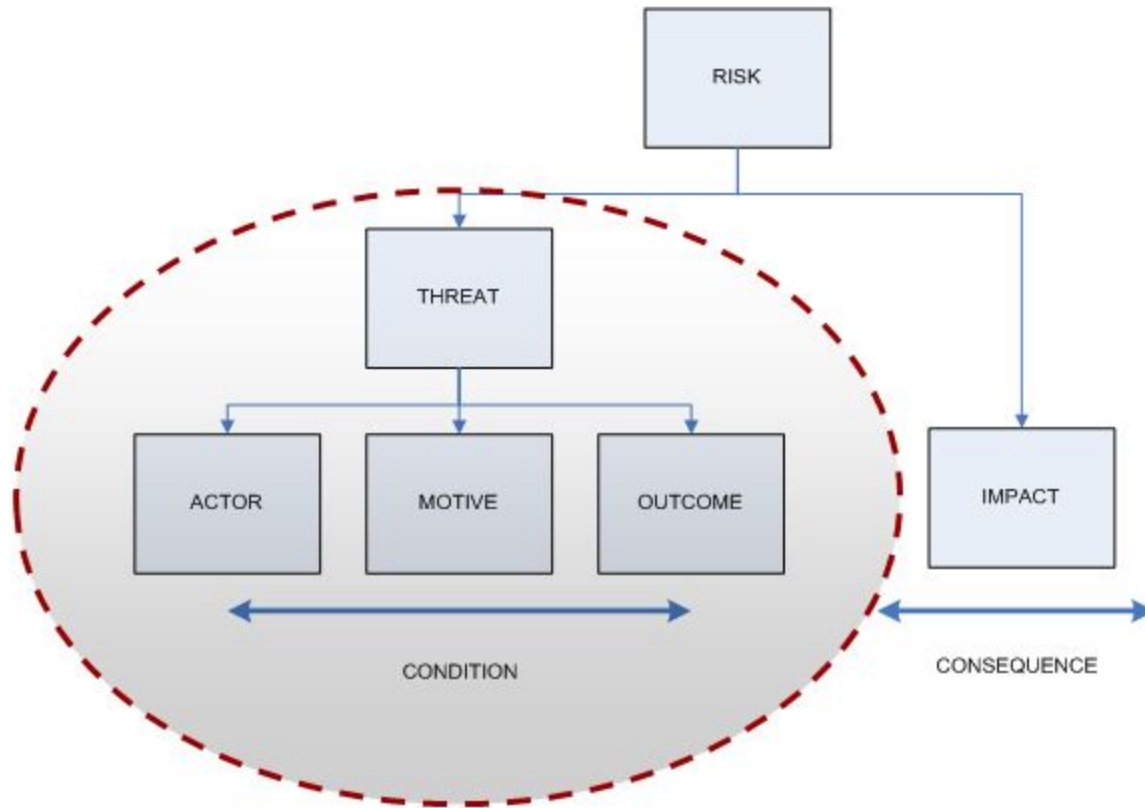
Threat describes the “condition” part of the risk equation.

Risk may not be present if there is no threat present (i.e., there is no vulnerability to exploit).

Threat Is a Part of Risk -2



Expanding the Threat Scenario



Real-world Threat Scenario -1

Sources of threats

- Deliberate actions by people (inside and outside the organization)
- Accidental actions by people (inside and outside the organization)
- System problems
- Other problems

Real-world Threat Scenario -2

Outcomes of threats

- Disclosure or viewing of sensitive information
- Modification of important or sensitive information
- Destruction or loss of important information, hardware, or software
- Interruption of access to important information, software, applications, or services

Information Asset Risk Profile

The information asset risk profile is used to capture threat, risk, and mitigation information for your information asset.

You will create a new risk profile for each area of concern that you capture and expand into a threat scenario.

Begins the risk assessment process

Narrows the risk assessment to only those situations that are plausible for you

Practice Exercise

Use the Information Asset Risk Environment Maps
(worksheets 9a, 9b, and 9c)

For each container on which your information asset lives

- Capture any areas of concern you have for that asset on that container and write them on worksheet 10
 - Remember that a single container may result in the identification of one or more areas of concern.

Complete Step 4, Activity 1 using worksheet 10

Book – *Managing Information Security Risks*

References

Identifying areas of concern

pp. 93-97

Impact descriptions

pp. 172-175

Step 4 Summary

Upon completion of Step 4, you will have

- Captured real-world areas of concern for your information asset
- Begun the process of documenting risks to your information asset

Preview of Step 5

Coming in Step 5

- Developing a more robust collection of threat scenarios for your asset and your organization by identifying the range of potential threat scenarios that are relevant to your information asset
 - What threat scenarios are relevant?
 - Human actors using network access
 - Human actors using physical access
 - Technical problems
 - Other problems



OCTAVE[®] Allegro Training

Step 5 – Identify Threat Scenarios

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

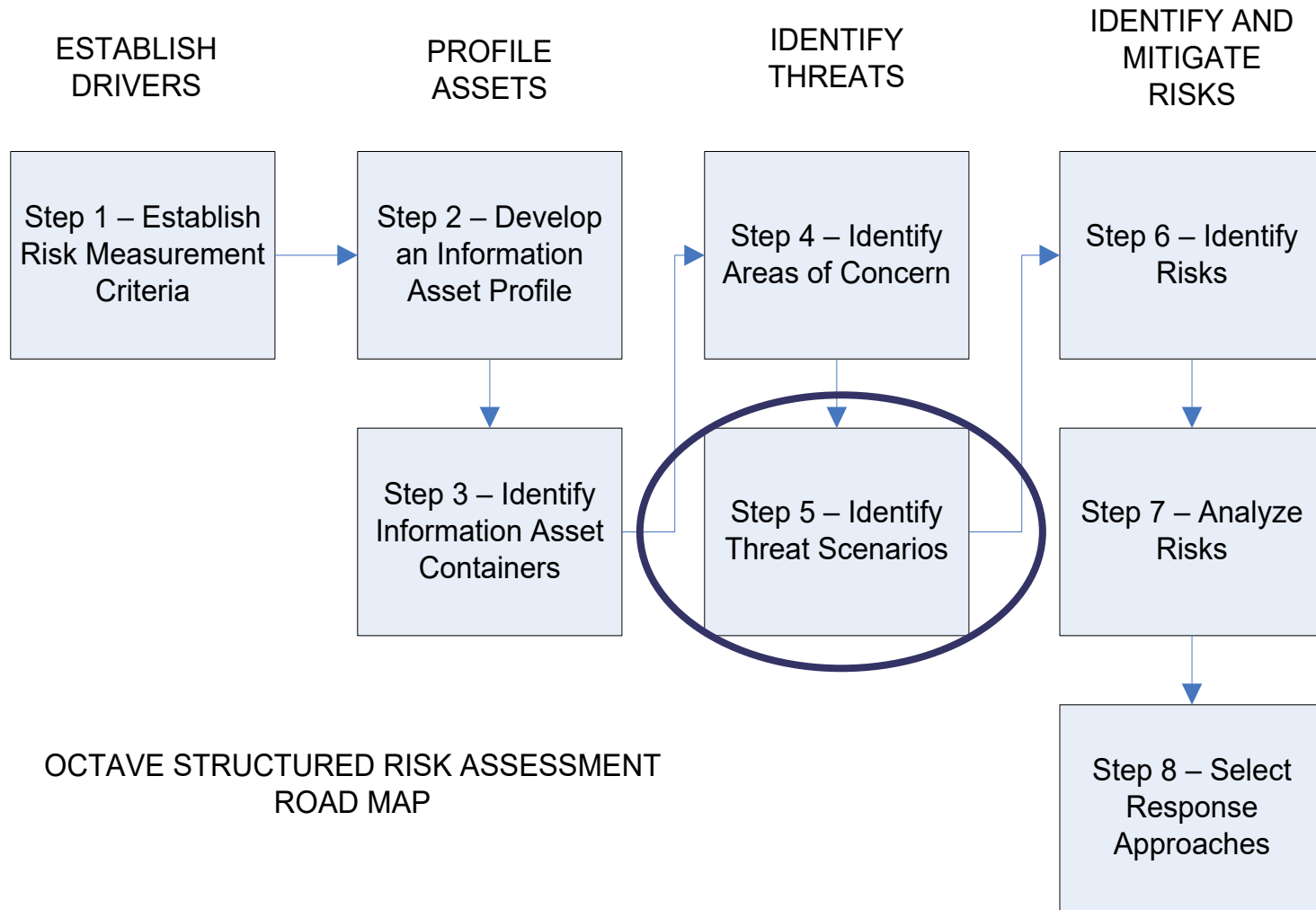
Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0487

OCTAVE Allegro Roadmap



OCTAVE STRUCTURED RISK ASSESSMENT
ROAD MAP

What Is a Threat?

A threat is an indication of a potential undesirable event.

- A situation or scenario involving a person or natural occurrence
- Resulting in an undesirable outcome

Origin/sources of Threats

Organizational and operational vulnerabilities from inadequate controls and practices

Technical vulnerabilities

Environment

People

Properties of a Threat

Actor (human or natural)

Motive (accidental or deliberate)

Access or Means (technical, physical)

Undesirable outcome (disclosure, modification, destruction or loss, interruption)

Outcomes of Threats

Disclosure or viewing of sensitive information

Modification of important or sensitive information

Destruction or loss of important information, hardware, or software

Interruption of access to important information, software, applications, or services

Threat Scenarios

A simplified way to consider situations in which an information asset can be compromised

Graphically represented in a standard set of paths known as a threat tree

Threat trees help you to consider a broad range of threats to your information asset.

Access (Optional)

Two types of access are considered.

1. Network – The primary or first means of gaining access to the critical asset is network based.
2. Physical – The primary or first means of gaining access to the critical asset is a physical means.

For example

- Using a stolen PC to access a network and steal confidential information is a *physical* attack – the theft of the PC.
- Using a home computer and the internet to break into a company's network and servers is a *network* attack.

Actors

Actors generally refers to humans but is also used on the System and Other threat trees to signify the general source of the problem. For example

- Hardware problems
- Acts of nature
- Fires

Motive (Optional)

Applicable only to the human actors using network or physical access

Two motives are considered.

1. Deliberate – Someone who chooses to attack or cause a problem
2. Accidental – Someone unknowingly causes a problem

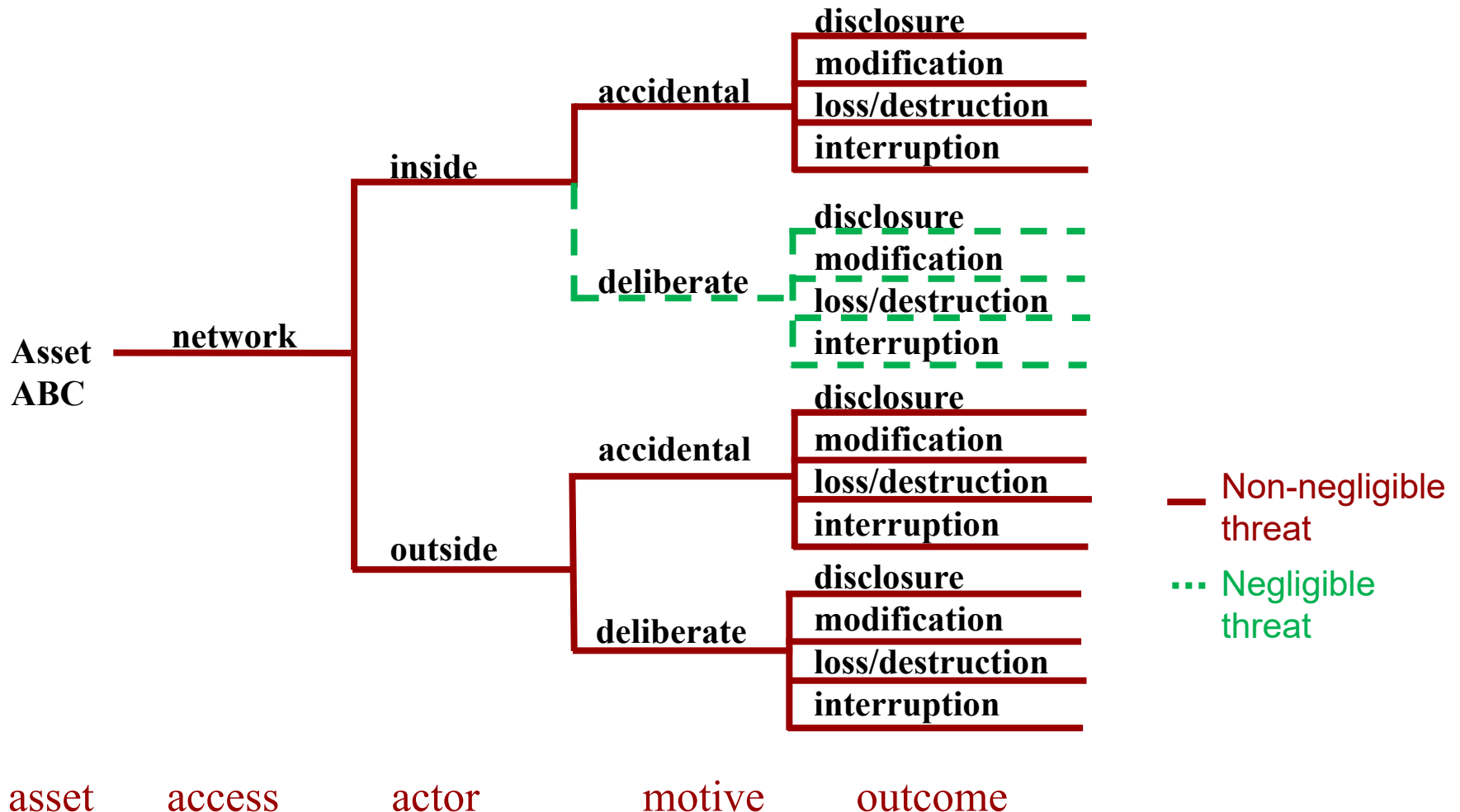
Threat Profile

A threat profile contains a range of threat scenarios (remember the areas of concern) for the following sources of threats and their outcomes.

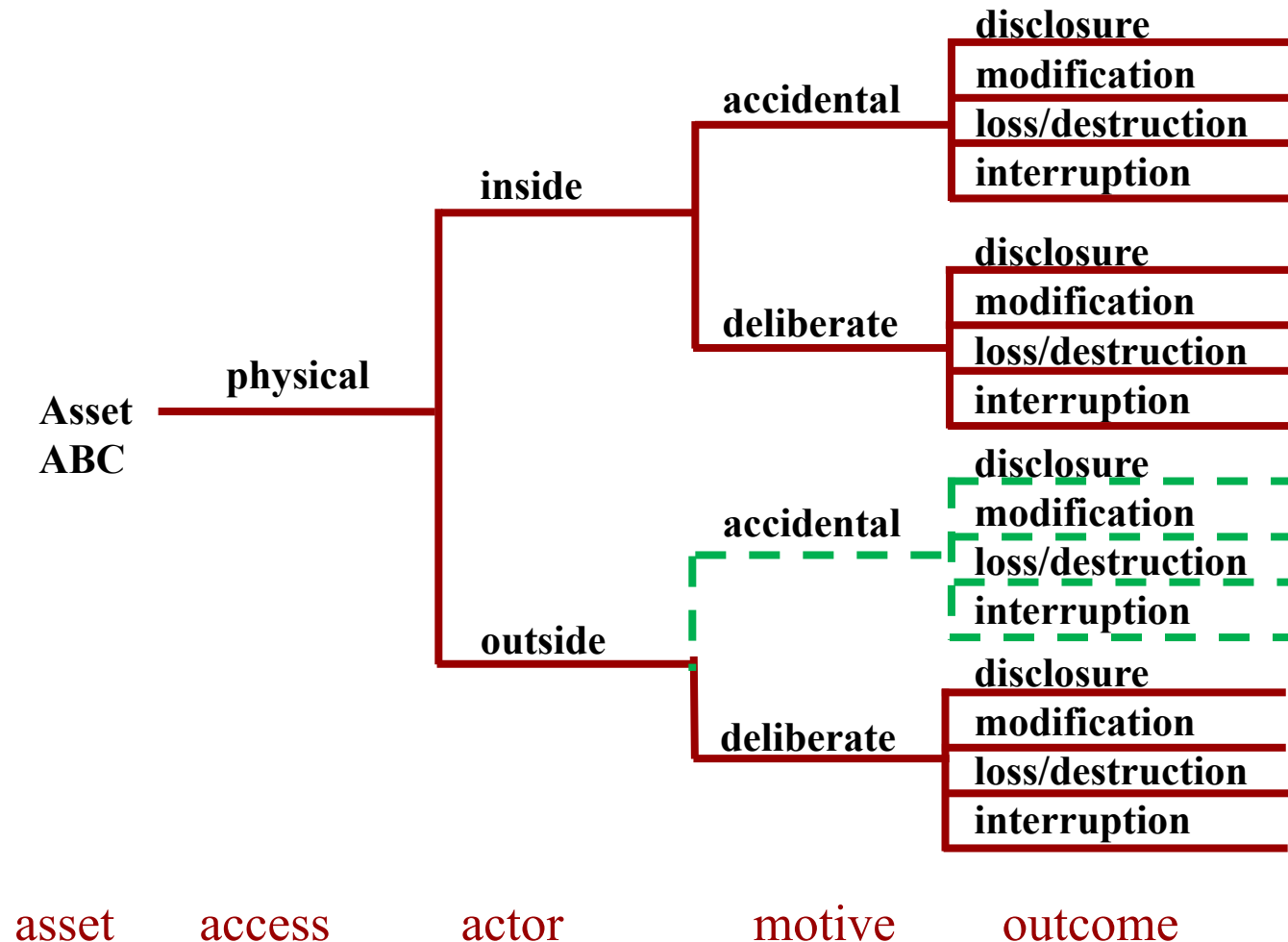
- Human actors using network access
- Human actors using physical access
- System problems
- Other problems

The threat profile is visually represented using asset-based threat trees.

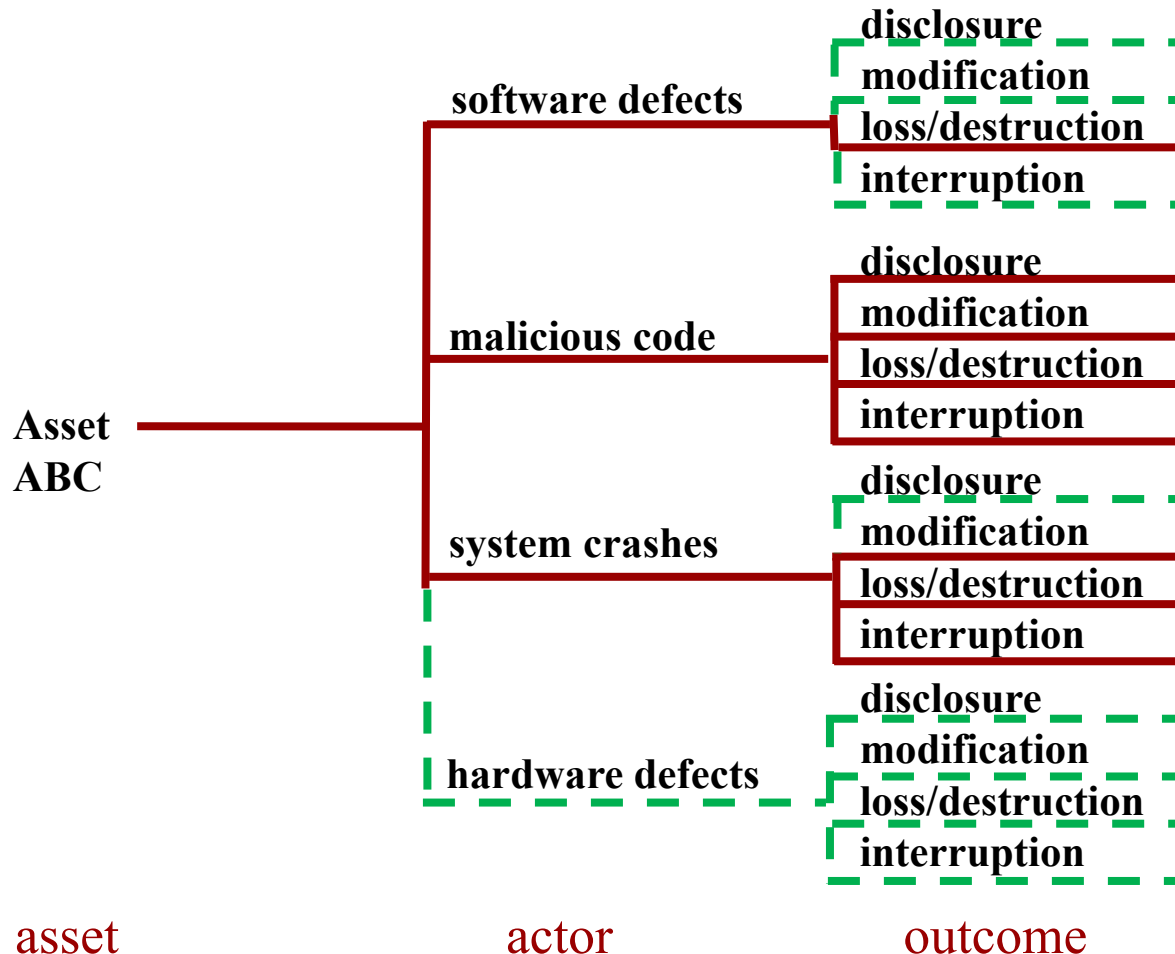
Example: Human Actors – Network Access



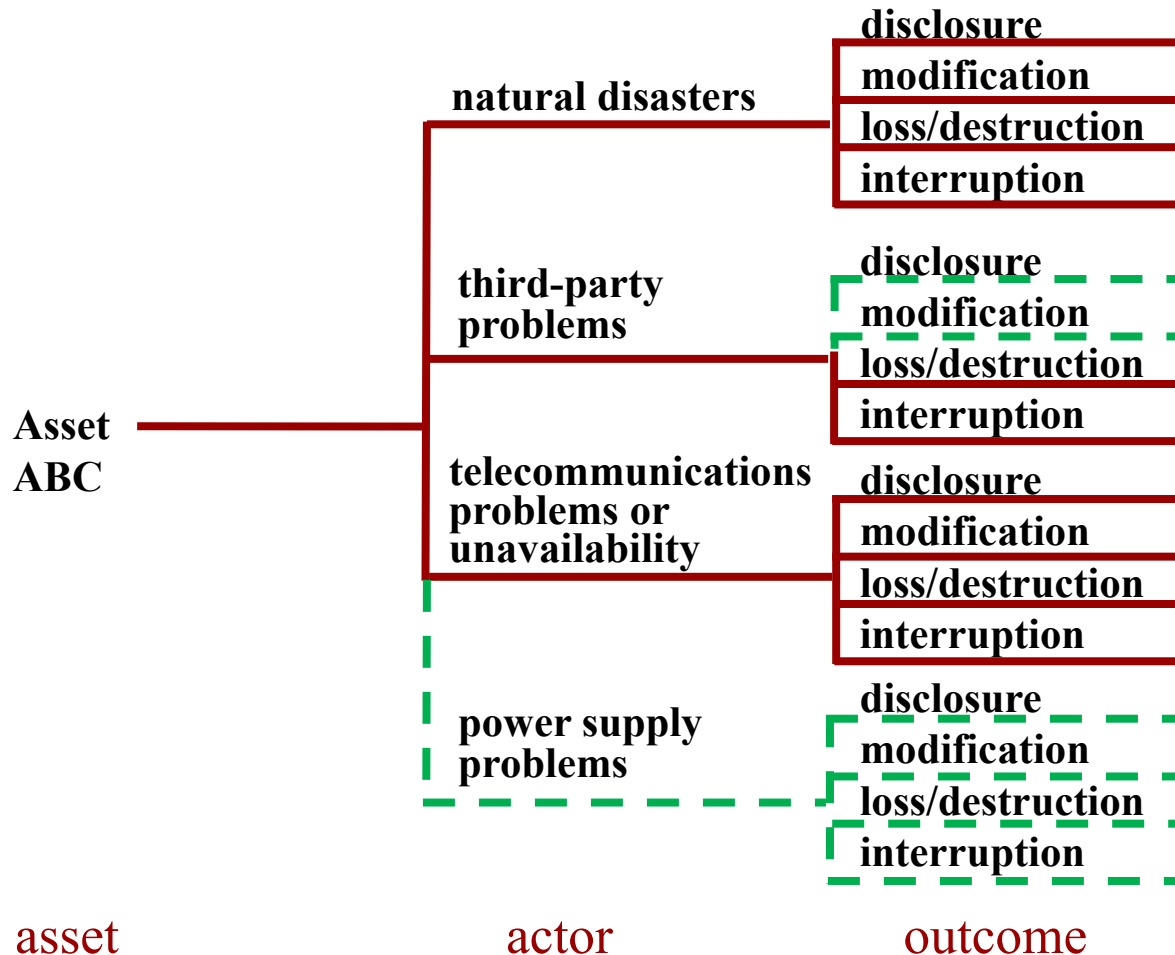
Example: Human Actors – Physical Access



Example: System Problems



Example: Other Problems



Threat Trees in OCTAVE Allegro

Areas of concern you developed correspond to branches in the threat trees.

To ensure a robust consideration of threats, each branch of the threat tree should be considered for your information asset.

Allegro simplifies this process by using scenario questionnaires.

Using Scenario Questionnaires

Questionnaires designed around containers

- Technical
- People
- Physical

A questionnaire should be considered for **each container** on which an information asset lives.

Questionnaires contain a collection of scenarios followed by questions designed to help seed the identification of additional threats.

Practice Exercise -1

Develop a robust set of threat scenarios for your information asset.

- Use Information Asset Environment Maps created in Step 4 (worksheets 9a, 9b, 9c).
- For each container and each container type complete the corresponding questionnaire.
- Remember that you may have more than one “yes” answer if there are different conditions, so circle more than one if necessary.

Complete Step 5, Activity 1 using Threat Scenario Questionnaires 1 - 3

Practice Exercise -2

Complete risk worksheets for each of the generic threat scenarios you identified on a questionnaire.

- For all “yes” answers on a questionnaire, record a new risk worksheet.
- If you find that you have answered “yes” to a question, but cannot come up with a corresponding real-life situation, move on.
- Continue until there is at least one worksheet completed for each “yes” answer on any questionnaire.

Complete Step 5, Activity 2 using Threat Scenario Questionnaires 1 - 3 and Worksheet 10

Optional Consideration

You may attempt to characterize the probability of the threat scenarios you have captured.

Probability can give you further information about whether a risk warrants response.

Cautions in Using Probability -1

Consider: What is the probability that your network will be hacked in the next month, 6 months, one year?

It is often difficult to characterize probability quantitatively for vulnerabilities and threats in the absence of data.

- Events are infrequent or never happened
- Events could be catastrophic (never imagined)

Cautions in Using Probability -2

The structured risk assessment uses descriptions which may include quantitative data if available.

- High
- Medium
- Low

If you decide to assign it, probability should be used for all threat scenarios.

Practice Exercise -3

If you decide to use it, characterize the probability of your threat scenarios by placing a “high,” “medium,” or “low” in the probability column on the risk profile.

Complete Step 5, Activity 3 using Threat Scenario Questionnaires 1 - 3 and Worksheet 10

Practice Exercise -4

In your teams, review the threats for the critical asset and map them to the threat trees.

Review all trees for threat gaps.

Book – *Managing Information Security Risks*

References

Identify threats pp. 128-136

Step 5 Summary

Upon completion of Step 5, you will have identified a robust collection of threat scenarios (and potential risks) that could occur in your organization and affect your information asset.

- Based on generic threat scenarios
- Articulated potential situations in your organization
- Provide the basis for considering impact if threats are realized, thereby completing the risk equation

Preview of Step 6

Coming in Step 6

- Identifying impact of realized threats
- Have you identified a risk for your information asset that may need to be mitigated?



OCTAVE[®] Allegro Training

Step 6 – Identify Risks

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

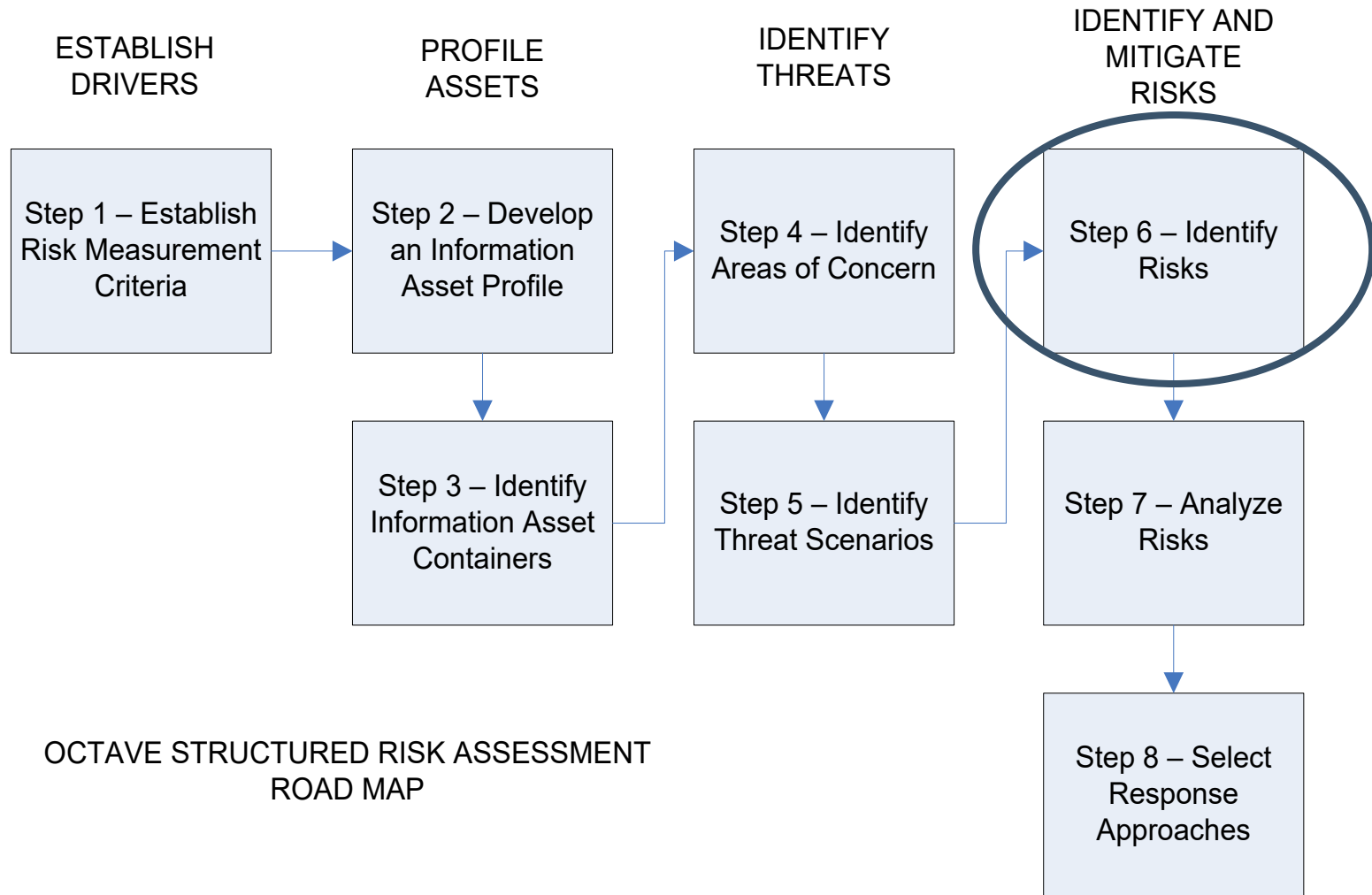
Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

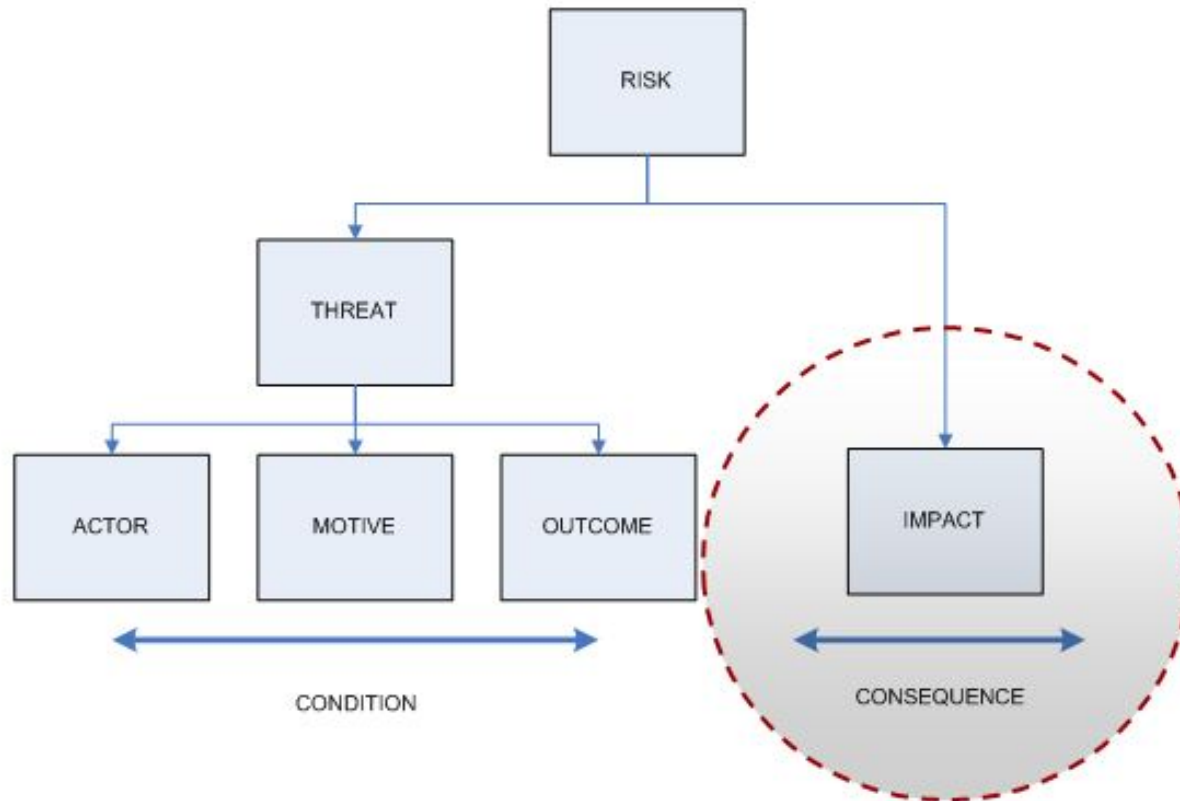
Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0487

OCTAVE Allegro Roadmap



Completing the Risk Equation



What Is a Risk? -1

A risk is the possibility of suffering harm or loss.

Refers to the situation where an event, incident, or occurrence brings about an undesirable outcome, resulting in a negative impact or consequence.

Composed of

- An event
- Uncertainty
- A consequence

What Is a Risk? -2

From a risk assessment perspective

- Risk describes the combination of a threat (condition) and an impact (consequence).
- Risk is the combination of an **area of concern** and an **impact statement**.

Characterizing Impact -1

Impact describes how the organization is affected as a result of a threat.

An **impact statement** is a descriptive statement that details specifically how an organization is affected when a threat is realized.

Impact statements are used in the structured risk assessment to identify the consequence of a threat.

Characterizing Impact -2

An impact statement can be described in terms of the impact areas used in the risk measurement criteria.

- Reputation/customer confidence
- Life/health of customers
- Fines/legal penalties
- Financial
- Productivity

Considering Security Requirements

A threat describes an **undesired outcome**.

An impact statement (or consequence) describes the **resulting effect on the organization as a result of the undesired outcome**.

Outcomes and the information asset's security requirements are linked.

Outcomes and Requirements -1

Threat Outcomes

Disclosure

Modification

Loss/Destruction

Interruption

Security Requirements

Confidentiality

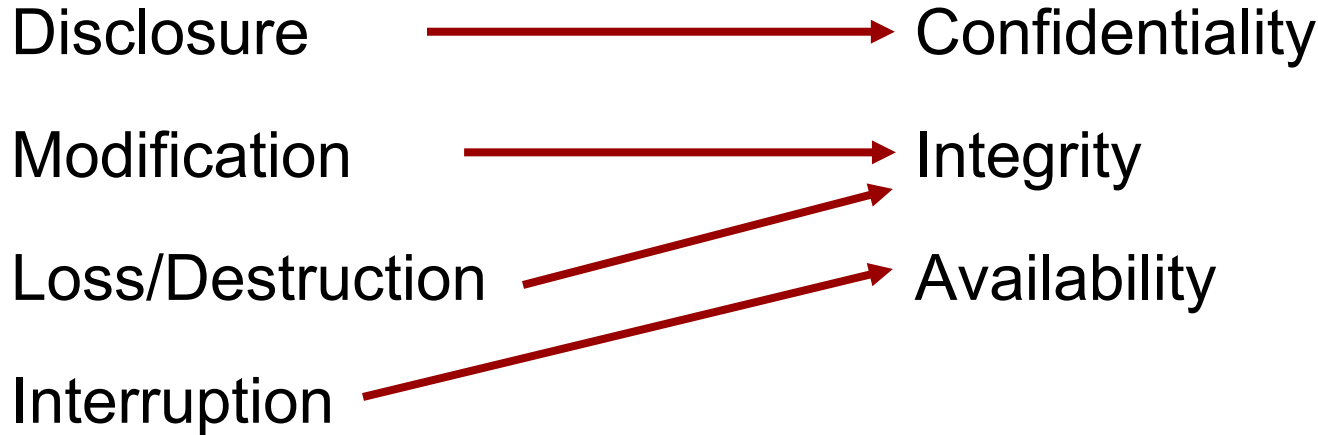
Integrity

Availability

Outcomes and Requirements -2

Threat Outcomes

Security Requirements



If you have already considered the outcome, you have also made an initial determination on security requirements.

Example Impact Statement -1

Area of concern

Incorrect file permissions enable a staff member to accidentally access another employee's medical records.

Impact statement

The medical records of an employee are disclosed, resulting in a lawsuit filed against the organization and a resulting fine of \$50,000. (The security requirement of confidentiality has been breached as a result.)

Example Impact Statement -2

Area of concern

Paper medical records are lost or destroyed due to a flood.

Impact statement

The medical records for a patient are not available for consultation to determine an appropriate treatment. The patient is given a drug to which they are allergic and is left permanently disabled. The patient sues the organization for \$25,000,000 and the hospital's reputation is irrevocably ruined. (The security requirement of availability has been breached as a result.)

Additional Examples

Personal employee information, including social security numbers, are disclosed, resulting in potential identity theft and a resulting lawsuit.

Widgets are not produced, resulting in a loss of production revenue of \$250,000 per day and potential that the company will be put out of business.

An incorrect dose of medication (or an incorrect medication) is given to a patient, resulting in their death, and resulting lawsuits, reputation damage, and possible fines.

Additional Considerations

Impact statements should

- Be as specific as possible
- Follow closely the impact areas in risk measurement criteria
- Be *quantitative* where possible
- Consider the security requirement

If you cannot develop an impact statement, your area of concern may not be plausible.

Practice Exercise

For each risk profile worksheet that you have created by capturing a threat scenario capture the list of possible consequences.

- Record one or more impact statements in the “Consequences” section of the Information Asset Risk Worksheet for each threat scenario you have created.
- Be as specific as possible – consider impact areas and be quantitative where practical.

Complete Step 6, Activity 1 using Worksheet 10

Step 6 Summary

Upon completion of Step 6, you have identified the potential impact of an area of concern.

- Identifies a risk for the information asset
- Provides a check on whether the area of concern is valid
- Completes the risk equation: condition + consequence

Preview of Step 7

Coming in Step 7

- Identifying extent of impact of a realized risk
- Evaluating and prioritizing risks in advance of response planning
- How extensively does the impact affect your organization?
- Which risks need to be addressed first?



OCTAVE[®] Allegro Training

Step 7 – Analyze Risks

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

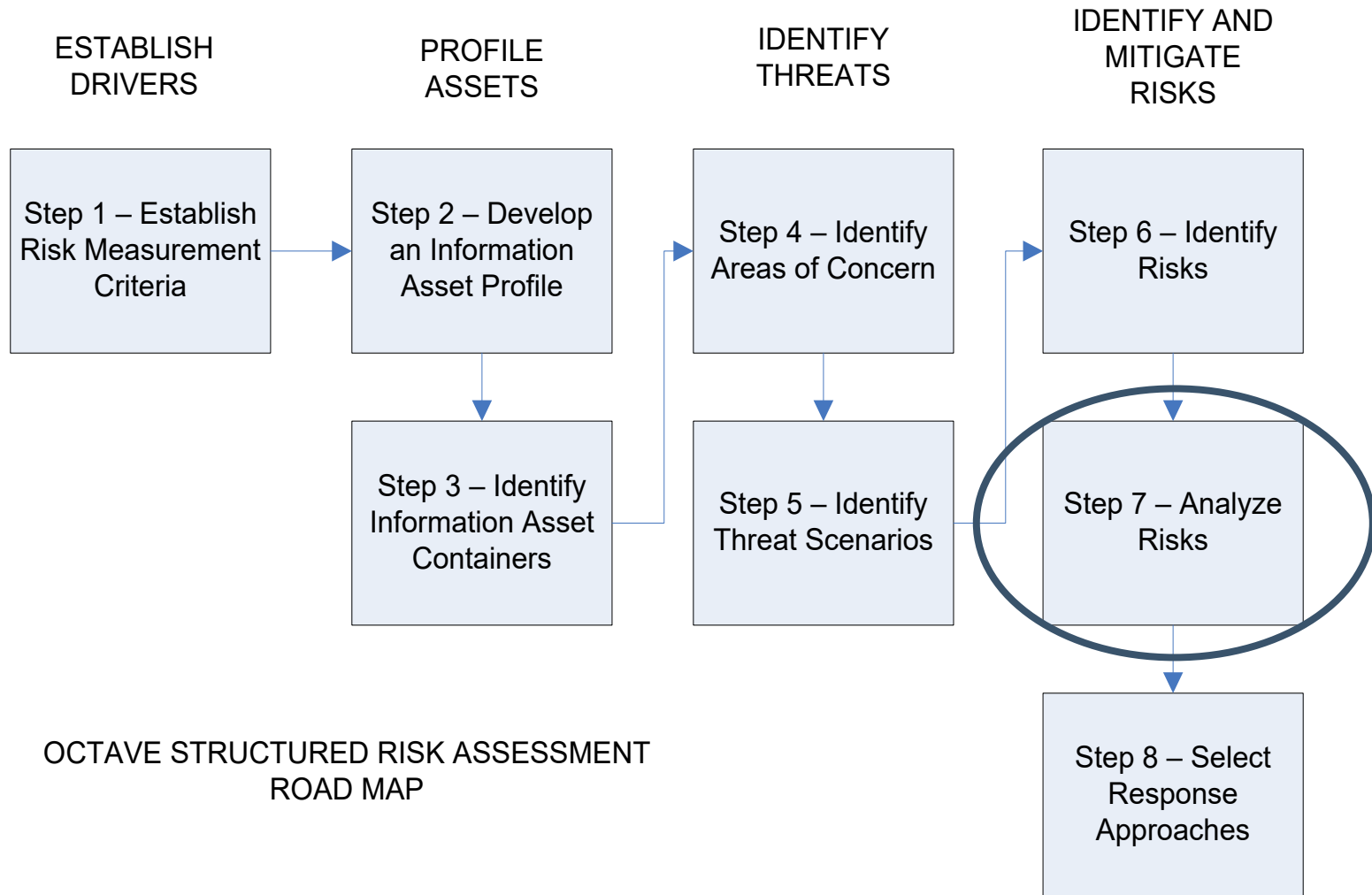
Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0487

OCTAVE Allegro Roadmap



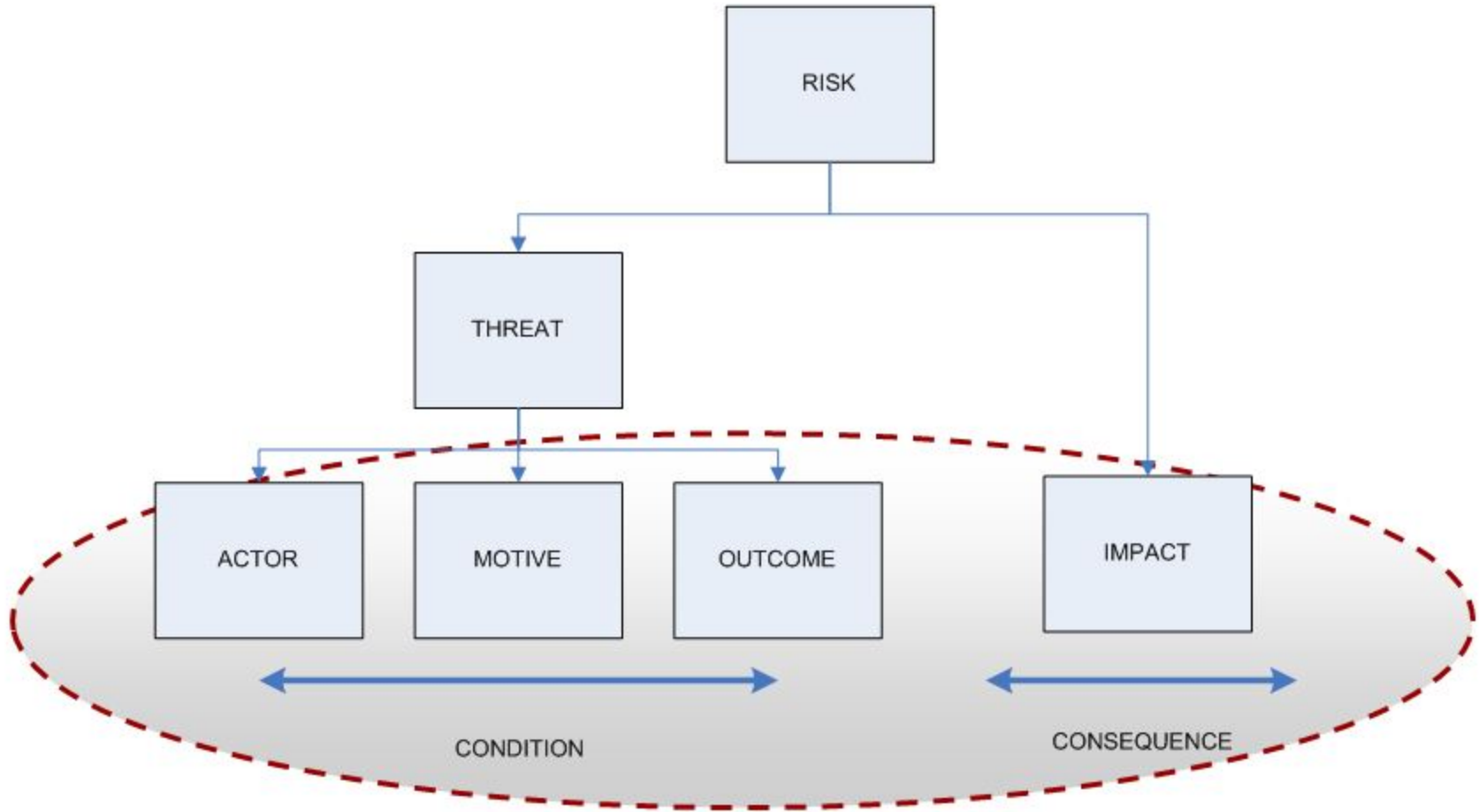
OCTAVE STRUCTURED RISK ASSESSMENT
ROAD MAP

Risk Analysis

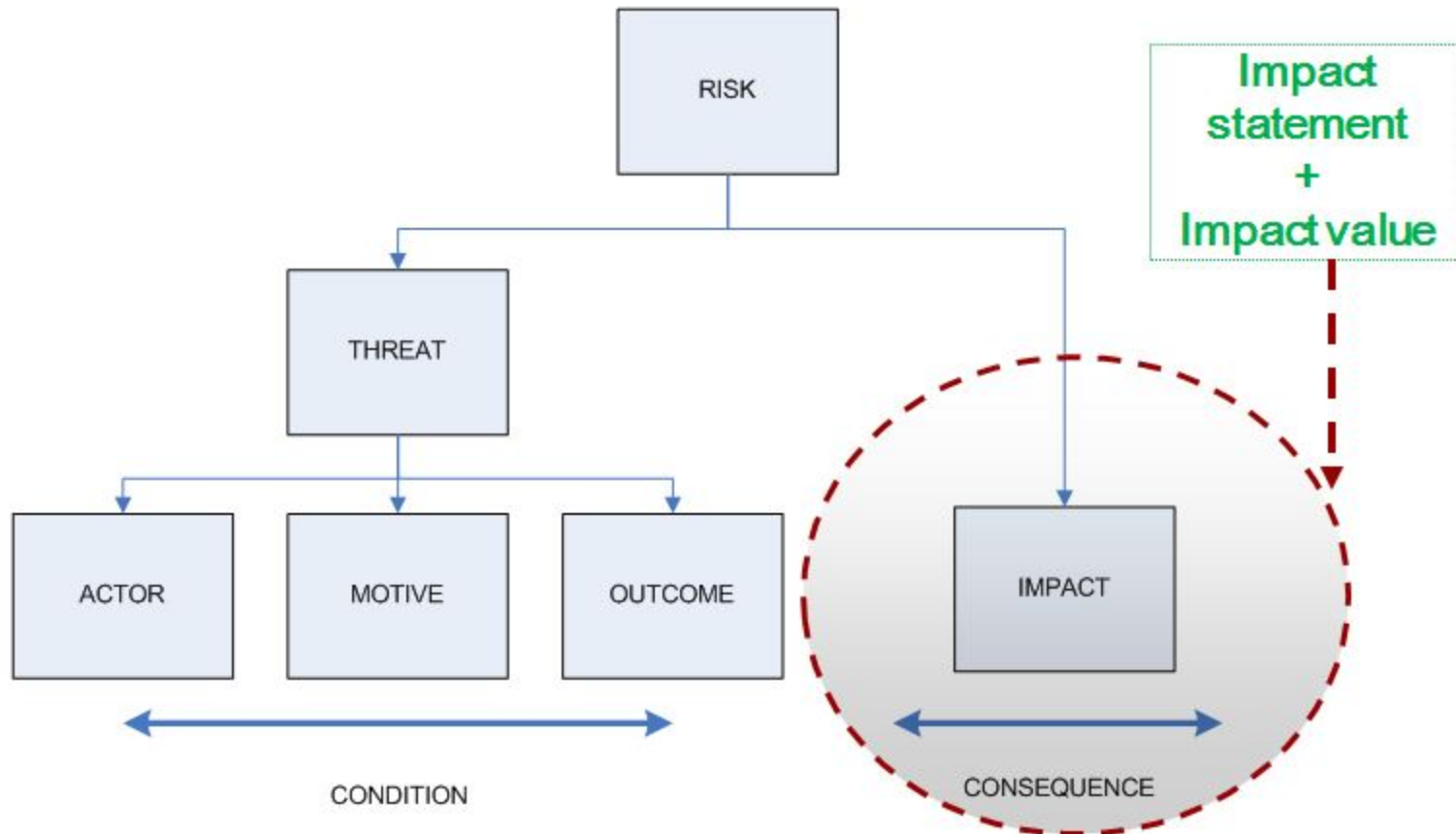
Risk analysis typically involves the following activities.

- Impact analysis
- Affinity grouping of risks for the purpose of realizing benefits in mitigation and control selection
- Prioritization of risks for mitigation

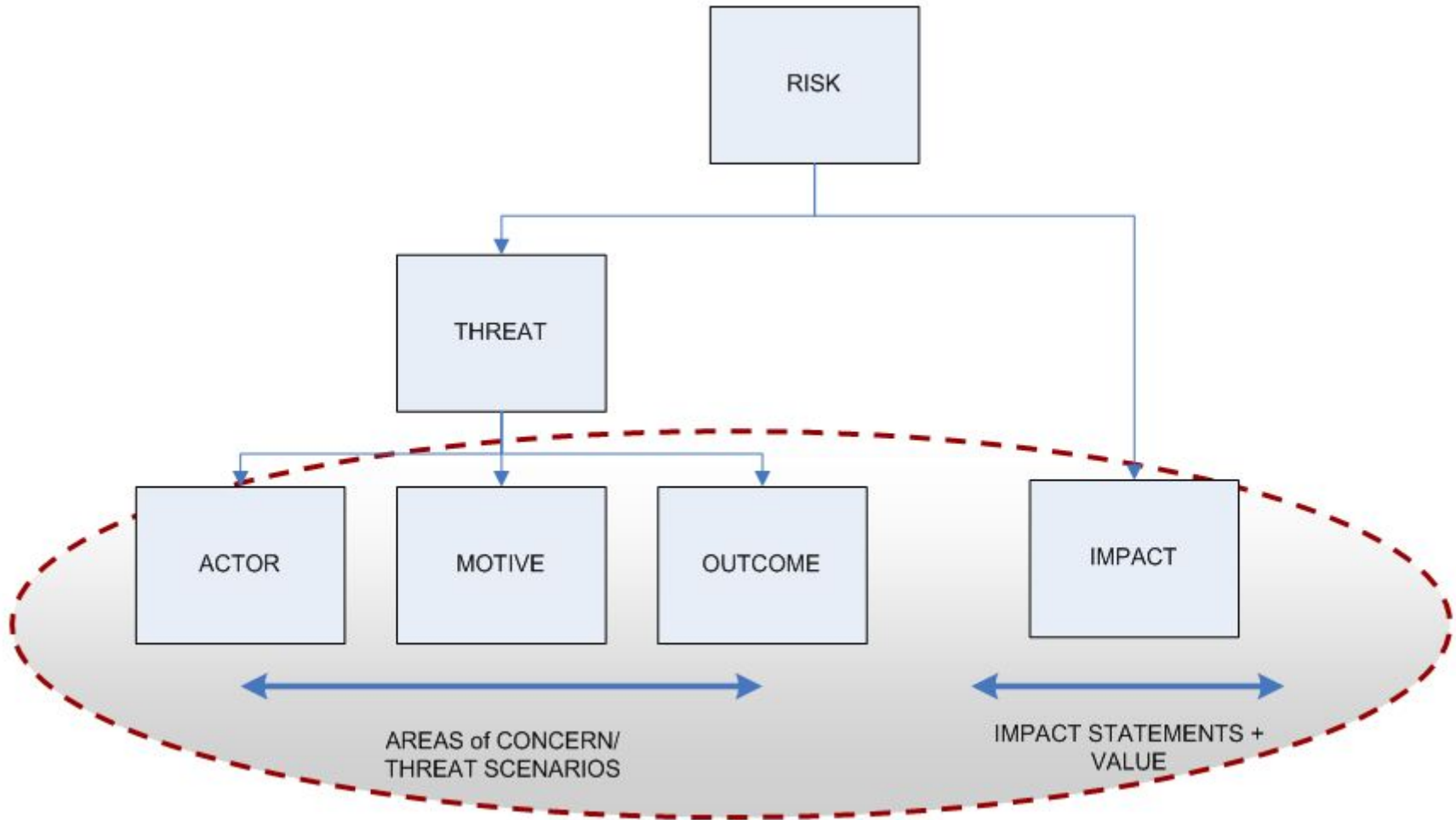
Risk = Condition + Consequence



Completing the Risk Equation



Risks Covered by Allegro



What Is an Impact Value?

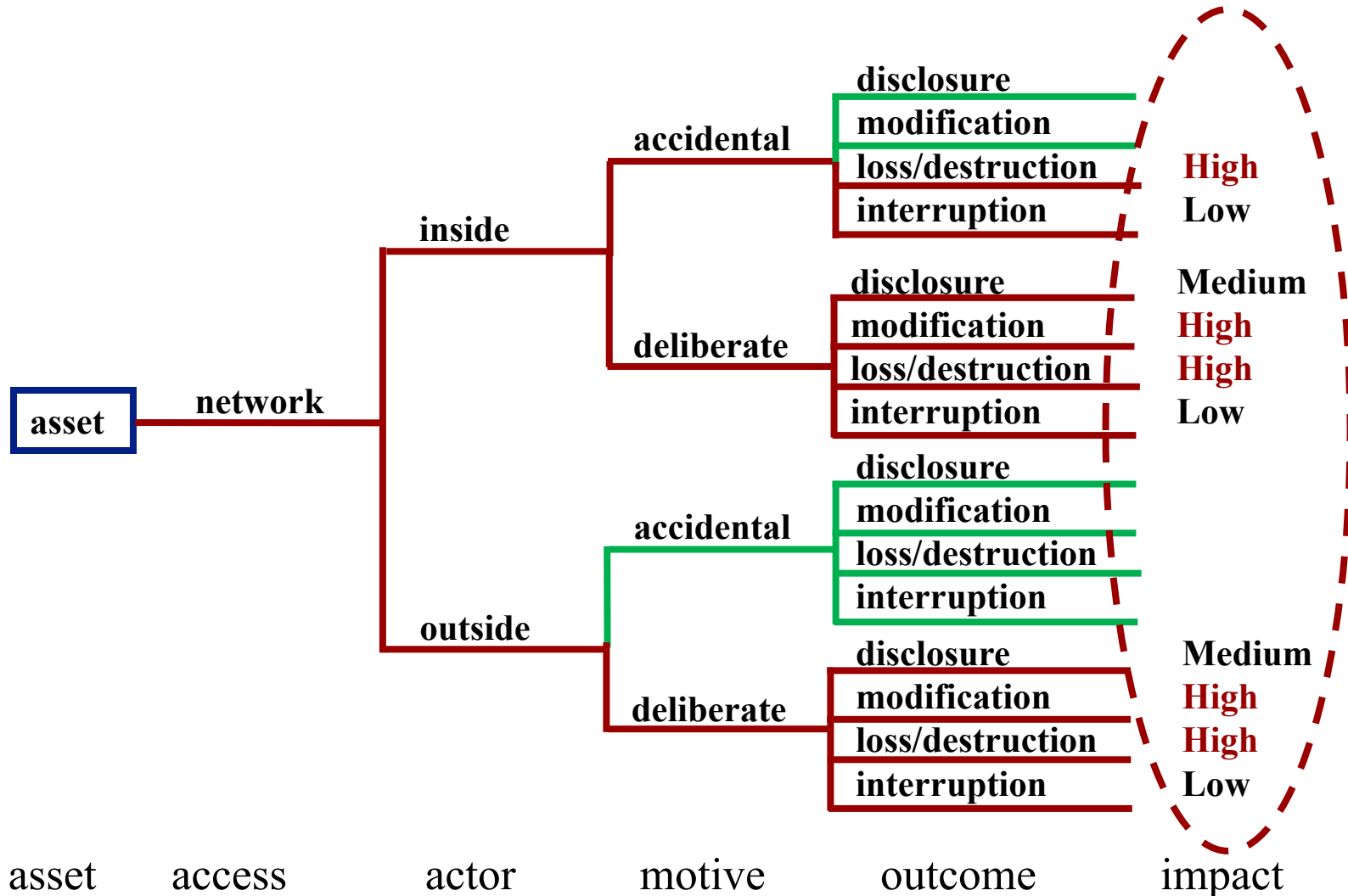
A quantitative or qualitative value assigned to describe the **extent** of impact to an organization.

The risk measurement criteria you developed is the basis for assigning the value.

Not all impacts are equal; impact value gives you a way to prioritize them using your risk measurement criteria.

Goal: Determine which risks need to be mitigated and in what priority.

Analyzing Risks



Using Impact Statements

In Step 1 you developed impact criteria and prioritized impact areas for your organization.

In Step 7 these criteria will help you to determine which risks are a higher priority ***to your organization***.

Risks which have a significant impact on your organization in the most significant areas are highest priority.

Relative Risk Score -1

The first step in the OCTAVE Allegro risk analysis process is computing a relative risk score.

The relative risk score is derived by considering the extent to which the consequence of a risk affects the organization as compared to the relative importance of the various impact areas.

By using these criteria, you are ensuring that risks are scored in the context of your organizational drivers.

Relative Risk Score -2

It is important to remember that

- Relative risk scores are only meant to be used for prioritization
- Higher-scoring risks are more significant than lower-scoring risks
- Differences between risk scores are not considered to be relevant

A Multi-step Process -1

Risk analysis is a multi-step process.

You must consider

- Area of concern (threat)
- Resulting impact (impact statement)
- Effect of impact in each impact area (impact value)
- Resulting severity of impact (impact value)
- Affect on security requirements

A Multi-step Process -2

1. Evaluate the impact in terms of the impact areas in your risk measurement criteria.
2. Resolve across impact areas to determine an overall impact value.
3. Use the impact statement to guide your choice.

Impact Area	Impact Value
Reputation	High
Financial	Moderate
Productivity	Moderate
Safety and Health	Low
Fines and Legal Penalties	High

A Multi-step Process -3

4. Compute the score for each impact area by multiplying the impact area rank by the impact value.
5. Total the score column. This total is the relative risk score.

Impact Area	Ranking	Impact Value	Score
Reputation	4	Moderate (2)	8
Financial	5	Low (1)	5
Productivity	3	Low (1)	3
Safety and Health	1	High (3)	3
Fines/Legal	2	High (3)	6
		Total Score	26

Example -1

Area of concern

Incorrect file permissions enable a staff member to accidentally access another employee's medical records.

Impact statement

The medical records of an employee are disclosed, resulting in a lawsuit filed against the organization and a resulting fine of \$50,000.

Example -2

Risk analysis – impact areas

- Lawsuit filed against the organization = **MODERATE**
- Fines of \$50,000 = **HIGH**
- Reputation is irrevocably damaged = **HIGH**
- Little to no health and safety impact = **LOW**
- Little to no productivity impact = **LOW**

Example -3

Impact Area	Ranking	Impact Value	Score
Reputation	4	High (3)	12
Financial	5	High (3)	15
Productivity	3	Low (1)	3
Safety and Health	1	Low (1)	1
Fines/Legal	2	Moderate (2)	4
		Total Score	35

Practice Exercise

Using your impact evaluation criteria as a guide, evaluate the magnitude of the impact for each of the risks you have identified. Decide which impacts cause a

- **High** consequence to your organization
- **Medium** consequence to your organization
- **Low** consequence to your organization

After evaluating each of the impact areas, use your impact area ranking to compute a relative risk score for each risk.

Complete Step 7, Activity 1 & 2 using Worksheet 10

Book – *Managing Information Security Risks*

References

Evaluate risks pp. 180-183

Step 7 Summary

Upon completion of Step 7 you have fully identified and analyzed the risks to your information asset.

Preview of Step 8

Coming in Step 8

- Identifying which approach to take in responding to each risk
- Which risks must be mitigated and which can be accepted or deferred?



OCTAVE[®] Allegro Training

Step 8 – Select Response Approaches

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

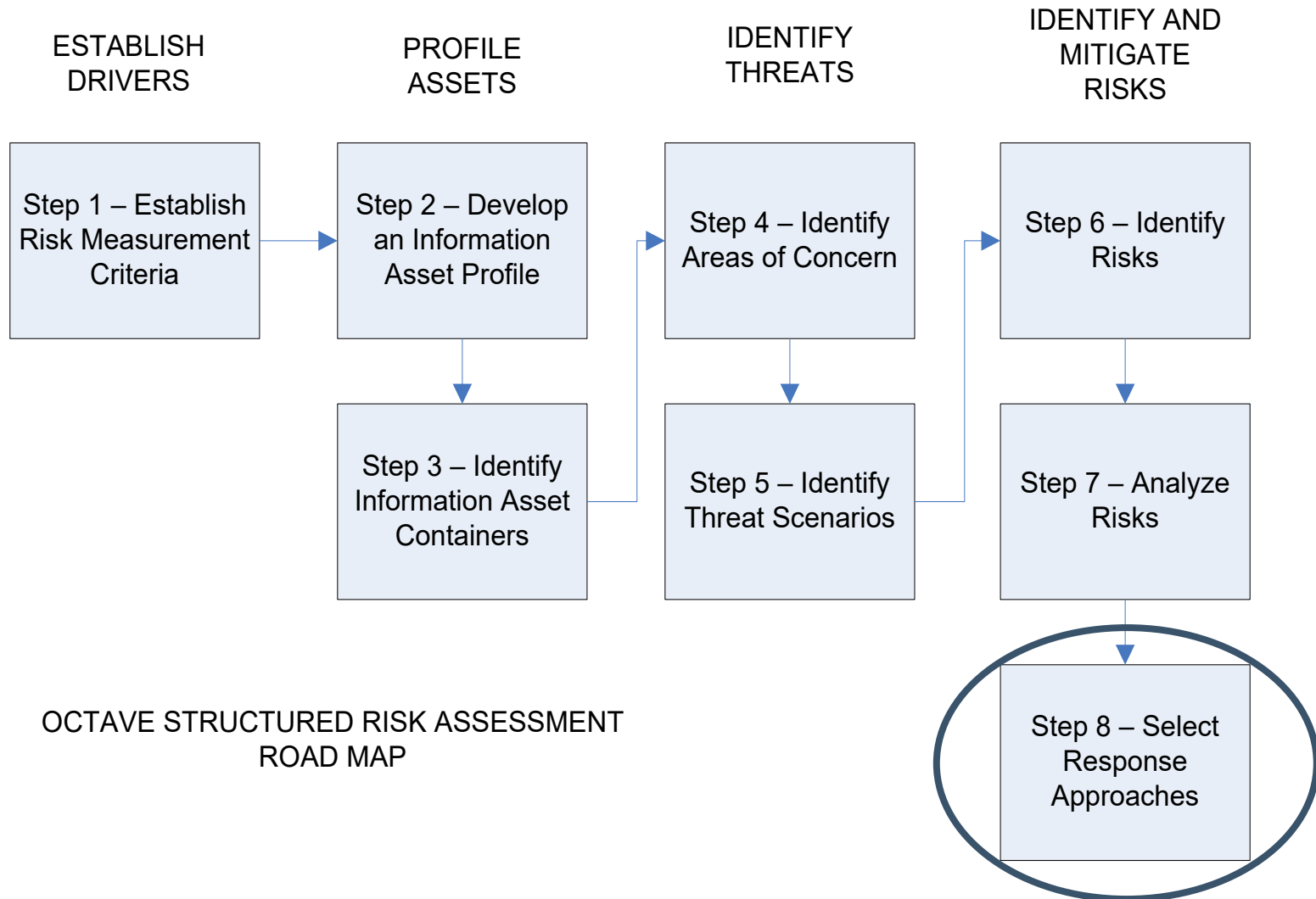
Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

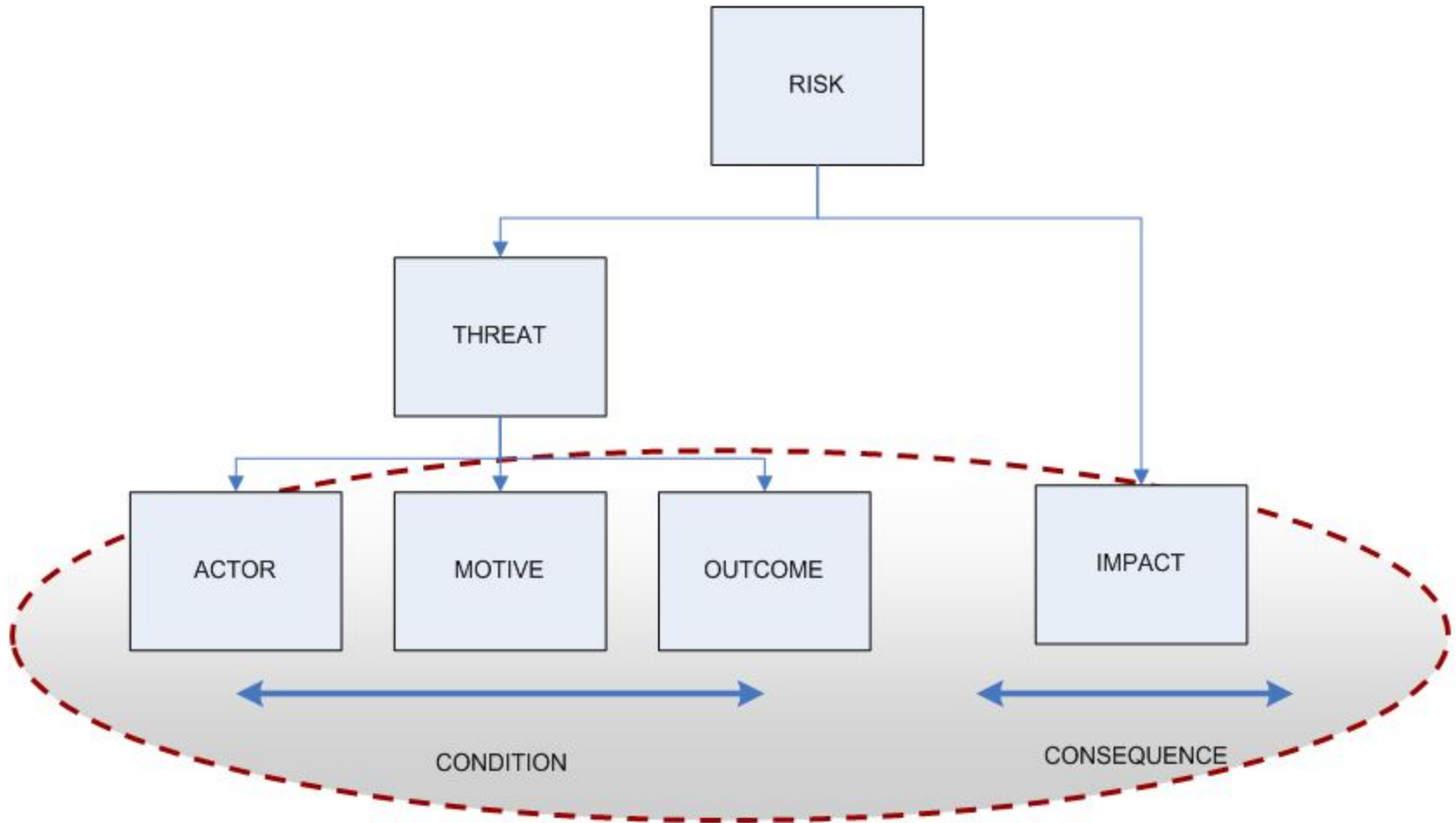
Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0487

OCTAVE Allegro Roadmap



Risk = Condition + Consequence



Risk Response Considerations -1

Your goal in risk response planning is to prioritize, evaluate, and implement the appropriate risk-reducing controls based on your risk assessment process.

Risk Response Considerations -2

Elimination of all risk is impractical or impossible – you must

- Use the least-cost approach
- Implement the most appropriate controls to reduce risk to an acceptable level
- Ensure minimal adverse impact on the information asset and organization

What Is a Risk Response?

A response approach is the way that an organization intends to address risk.

Allegro provides three options.

1. Accept or assume
2. Defer
3. Mitigate

There are also other options for addressing risk.

Each option brings a separate course of action.

Accept or Assume Risk

Accepting the risk means that you continue to operate the information asset.

If your risk is high or medium, this is not an option (unless it is cost-prohibitive to mitigate).

For a low risk, you will monitor the risk and take action at a later time if necessary.

Defer Risk

Deferring risk means that you are neither accepting or mitigating the risk, but it is not an immediate priority.

Additional information is needed to determine which course to take.

- **Risk planning** – To manage risk by developing a risk response plan that prioritizes, implements, and maintains controls
- **Risk research and acknowledgement** – To lower the risk of loss by acknowledging the vulnerability and researching controls to correct the vulnerability

Mitigate Risk -1

You must act to mitigate all high and medium risks (unless it is cost-prohibitive to do so).

Two courses can be taken.

1. **Risk avoidance** – To avoid the risk by eliminating the risk cause/condition and/or consequence
2. **Risk limitation** – To limit the risk by implementing controls that minimize the adverse impact of the exploitation of a vulnerability by a threat

Usually, BOTH are required to some degree.

Mitigate Risk -2

Two considerations you must make in mitigating risks: **Cost-benefit** and **residual risk**.

- The mitigation strategy you choose must ultimately cost less than the loss you would sustain if the risk is realized.
- A mitigation strategy may not avoid, limit, or mitigate all of the risk. The remaining risk, called **residual risk**, must be identified and addressed.

Residual and Acceptable Risk

Residual risk is the potential for the occurrence of an adverse event after adjusting for the effectiveness and impact of all implemented security controls.

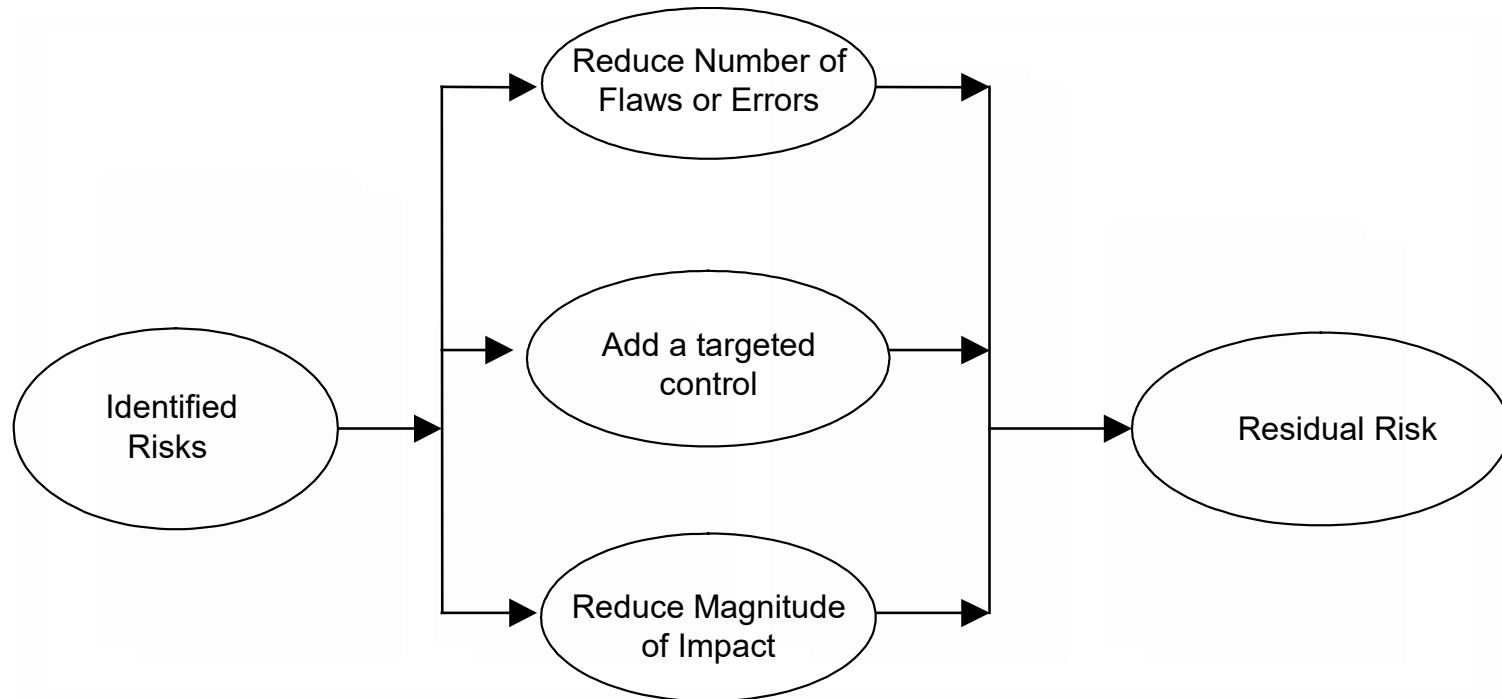
Acceptable risk is the level of risk that has been determined to be a reasonable level of potential loss/disruption to a system or organization.

Residual Risk

Technical (Supporting, prevention, detect & recover)

Management (Training, plans, procedures, ...)

Operational (Physical, personnel, backup, ...)



Another Option – Transfer Risk

You transfer the risk by using other options to compensate for the loss.

You may only transfer risk (rather than mitigate it) if you have someone willing to accept it.

YOU STILL RETAIN RESPONSIBILITY FOR THE RISK.

More Analysis May Be Needed

Relying upon the impact value may not be enough to determine what action to take for each risk.

You may need to create a risk matrix and scale.

This helps you better determine the severity of the risks you have identified.

It also provides a quantitative means to prioritize risks.

Categorize Risks

There are many ways for an organization to categorize its risks.

One straightforward method is to begin by simply sorting the risks in order from highest to lowest, dividing risks into pools.

If your organization is using probability you might want to consider developing a risk matrix to categorize the risks you have identified.

A Risk Matrix

	Risk Score		
Probability	31-45	16-30	1-15
High	POOL1	POOL2	POOL2
Medium	POOL2	POOL2	POOL3
Low	POOL3	POOL3	POOL4

Scale: High (>50 to 100) Medium (>10 to 50) Low (1 to 10)

Risk Drives Response Approach

Assign a response approach to each of your pools.

Remember that a decision about a response approach is highly dependent on your organization's unique operating circumstances.

Pool	Response Approach
POOL1	Mitigate
POOL2	Mitigate or Defer
POOL3	Defer or Accept
POOL4	Accept

Practice Exercise -1

Sort your risks by their relative scores and then divide the risks into categories.

If you are using probability then create a risk matrix to help categorize your risks.

Assign a disposition strategy to each category of risk.

Risks with a “high” value are most certain candidates for a “mitigate” strategy.

Be sure to consider whether your organization can accept any consequences related to the risk.

Complete Step 8, Activities 1 & 2 using Worksheet 10

Practice Exercise -2

Develop a strategy for all risks that require a response.

Consider

- Cost of the response strategy
- Layering of controls (administrative, technical, physical)
- The container(s) on which the information asset lives (Your mitigation activities must be focused at the container level to be effective.)

Complete Step 8, Activity 3 using Worksheet 10

Book – *Managing Information Security Risks*

References

Mitigation plans	pp. 209-216
Protection strategy	pp. 202-207
Strategic and operational practices	
Action items	pp. 218-220

Step 8 Summary

Upon completion of Step 8 you have fully articulated risks to your information asset and have decided upon an initial response strategy for each.



OCTAVE[®] Allegro Training

Summary and Next Steps

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon®, CERT®, CERT Coordination Center® and OCTAVE® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0487

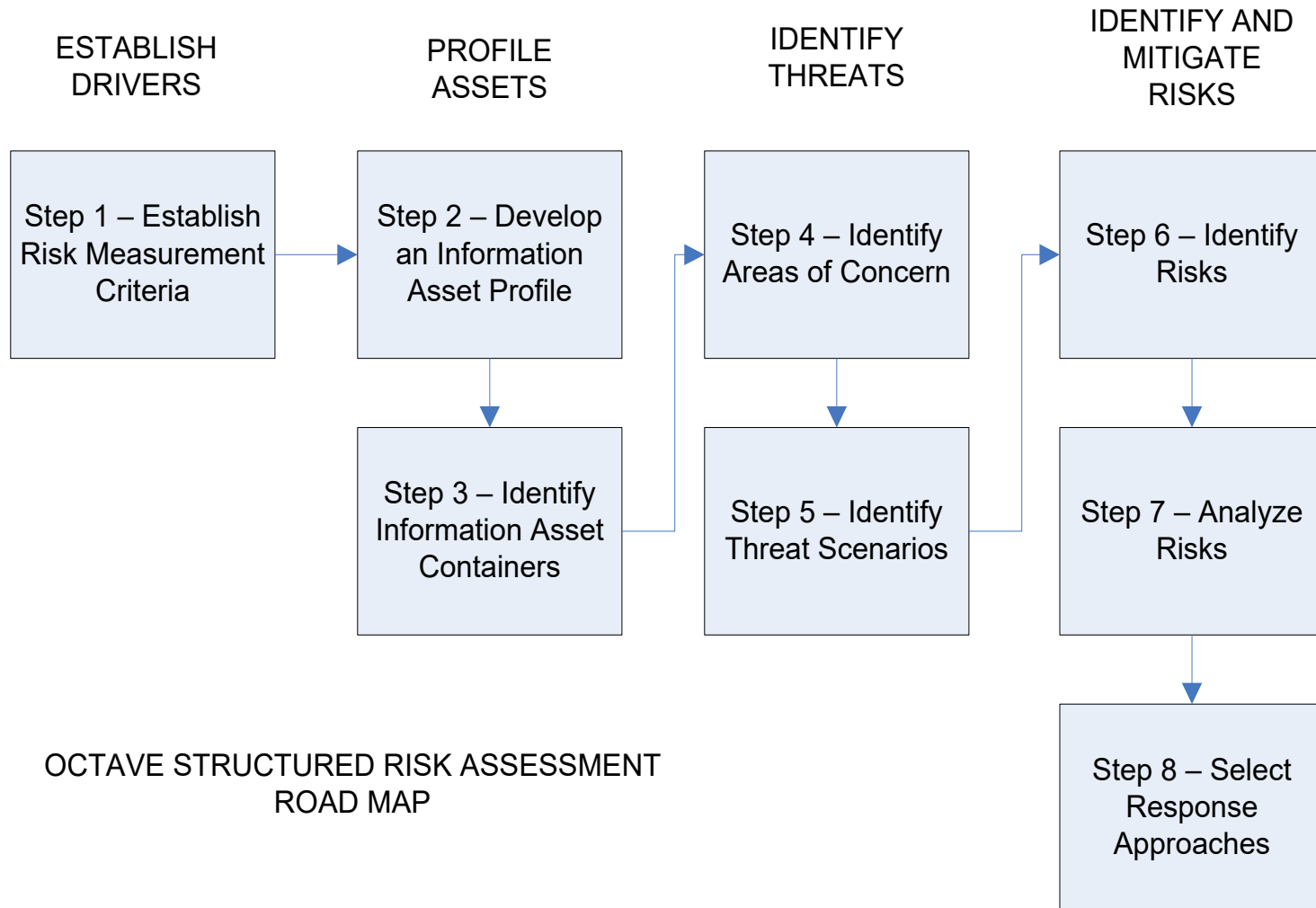
Purpose

Review key points of the course

Answer your questions

Provide feedback on this offering

OCTAVE Allegro Roadmap



OCTAVE STRUCTURED RISK ASSESSMENT
ROAD MAP

Outputs of the Allegro Process

Information asset profile for critical assets

Risk profile for information assets

- Relevant/contextual threat scenarios
- Prioritized risks
- Potential impacts
- Response strategies for high-priority risks

Discussion – Using the Results

What will you do with the results of the Allegro structured risk assessment?

How could you incorporate these results into

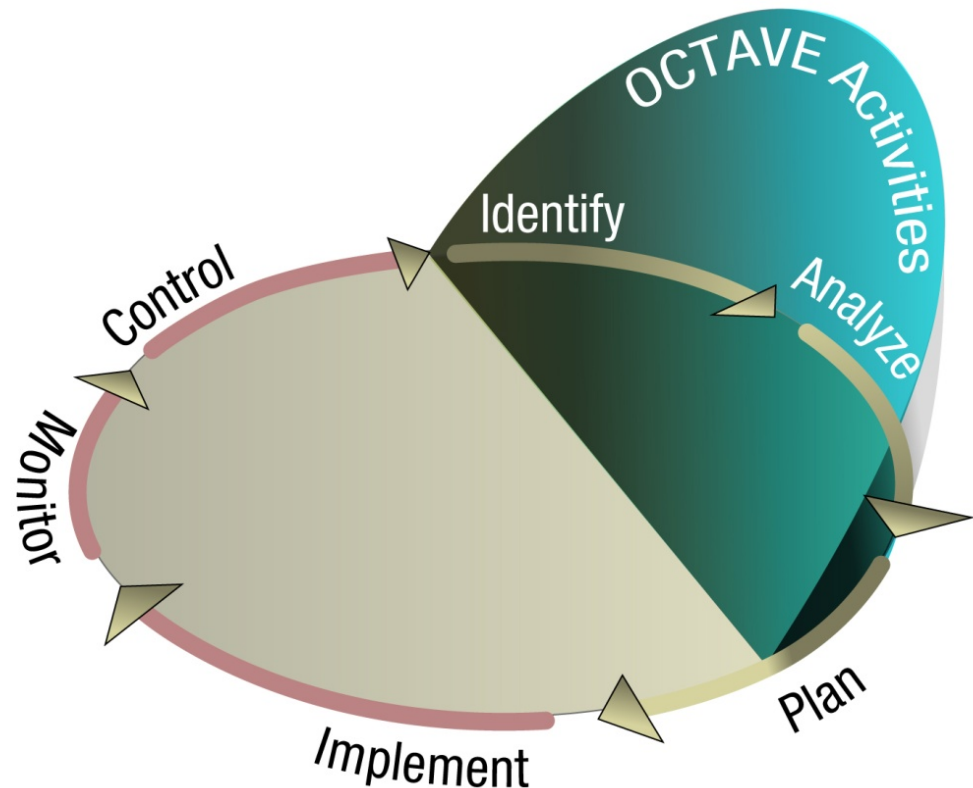
- Organizational, line of business, business unit, or departmental practice and procedures?
- Organizational security strategy and plans?
- Other organizational initiatives?
- Other audits and compliance checks?

What Do Senior Managers Need to Know?

Review and discuss the example Widget Company presentation.

OCTAVE Allegro Approach

OCTAVE is critical component of a risk management approach to information security.



Other OCTAVE Information

Updates to methods and other material will be periodically made available via the Web.

<http://www.cert.org/resilience/>

Send email to octave-info@sei.cmu.edu

Feedback to the SEI

What worked and what did not work

Tailoring

- What?
- Why?
- Was it successful?

Data or results: real or scrubbed

If you're willing to share your experiences with us, send email to octave-info@sei.cmu.edu

Key Points for the Course

Information security risk evaluation is more than a technology-based vulnerability assessment.

Services, business processes, assets

Understand how the organization's business goals are affected by risks

What key points did *you* get from this course?

Course Evaluation

Fill out and hand in the Course Evaluation Form before you leave.

How can this course be improved?

What worked well for you?

Any questions?

For Additional Information

Telephone 412/268-5800

Fax 412/268-5758

Internet customer-relations@sei.cmu.edu
octave-info@sei.cmu.edu

WWW <http://www.cert.org/resilience/>

U.S. Mail Customer Relations
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

After Step 8...

Complete all Allegro activities for selected asset – share results with owners, custodians, and stakeholders

Comparison and analysis of results across multiple assets

Review of recommended response efforts to realize efficiencies and eliminate redundancy

Pursue investment in selected controls and actions

Routinely monitor implementation progress and effectiveness of mitigation plans and selected controls

Monitor information security risks, looking for new risks and changes to existing risks

Questions?
