Evaluating CSIRT Operations

FIRST 2006

CERT® Training and Education
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Overview of Tutorial

Introduction

Evaluation Background

- Purpose
- Criteria
- Outcomes

Methods

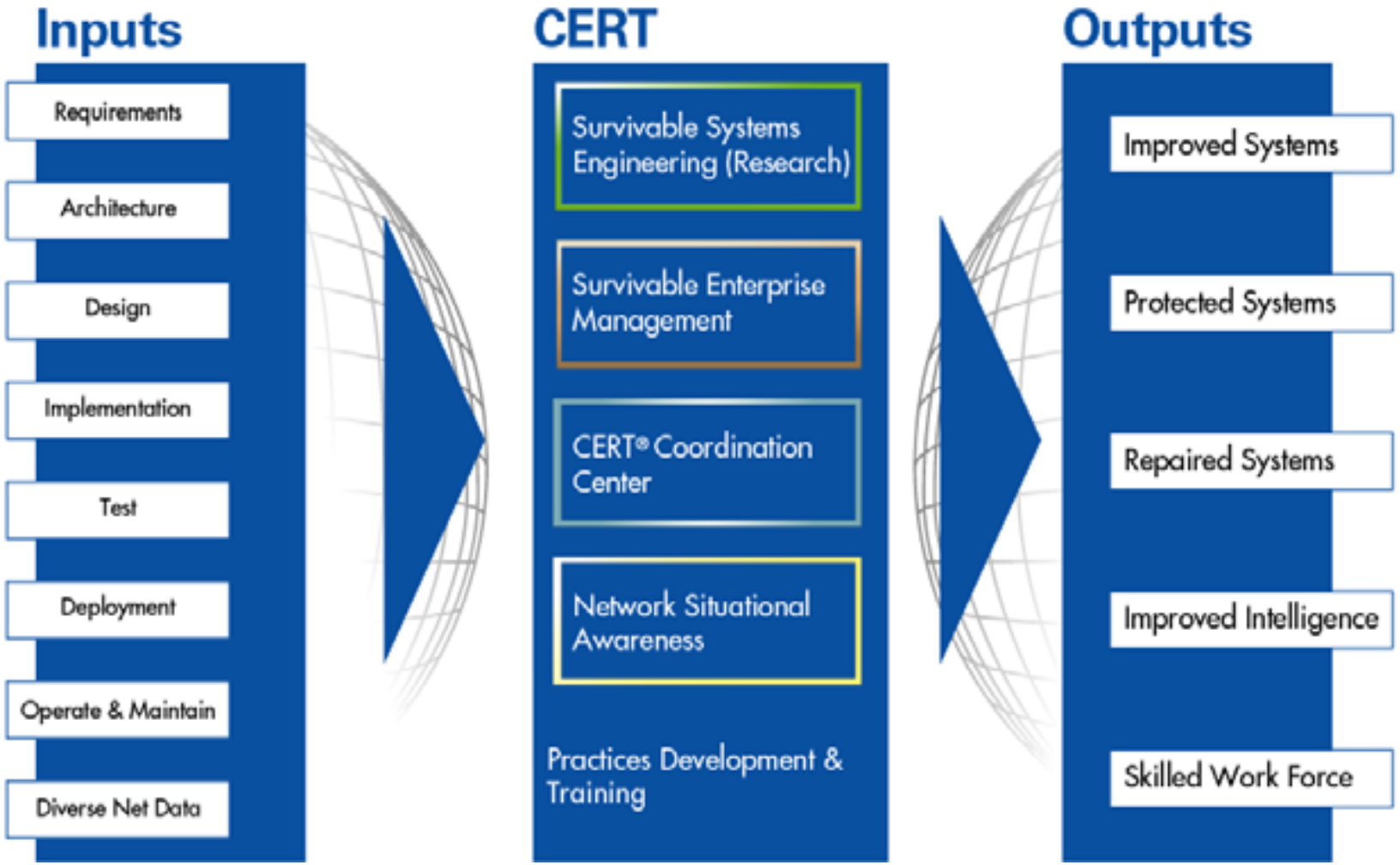
- GAP Analysis
- Mission Assurance Analysis Protocol (MAAP)
- Computer Network Defense (CND) Metrics Assessment
- Mission Diagnostic Tool

Summary

Introduction

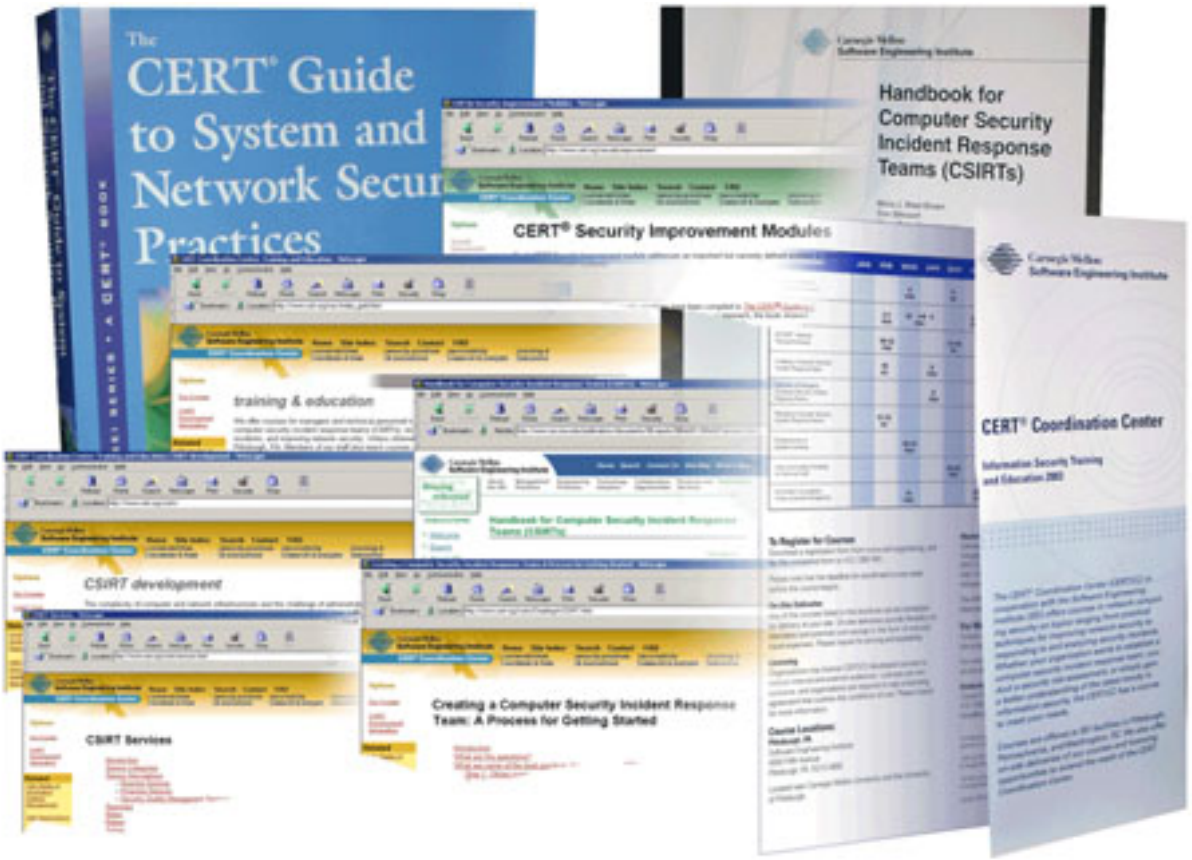
CERT® Program

It's important to address security issues at all phases of the systemsdevelopment life cycle. The CERT Program helps network administrators and managers address these issues.



CERT

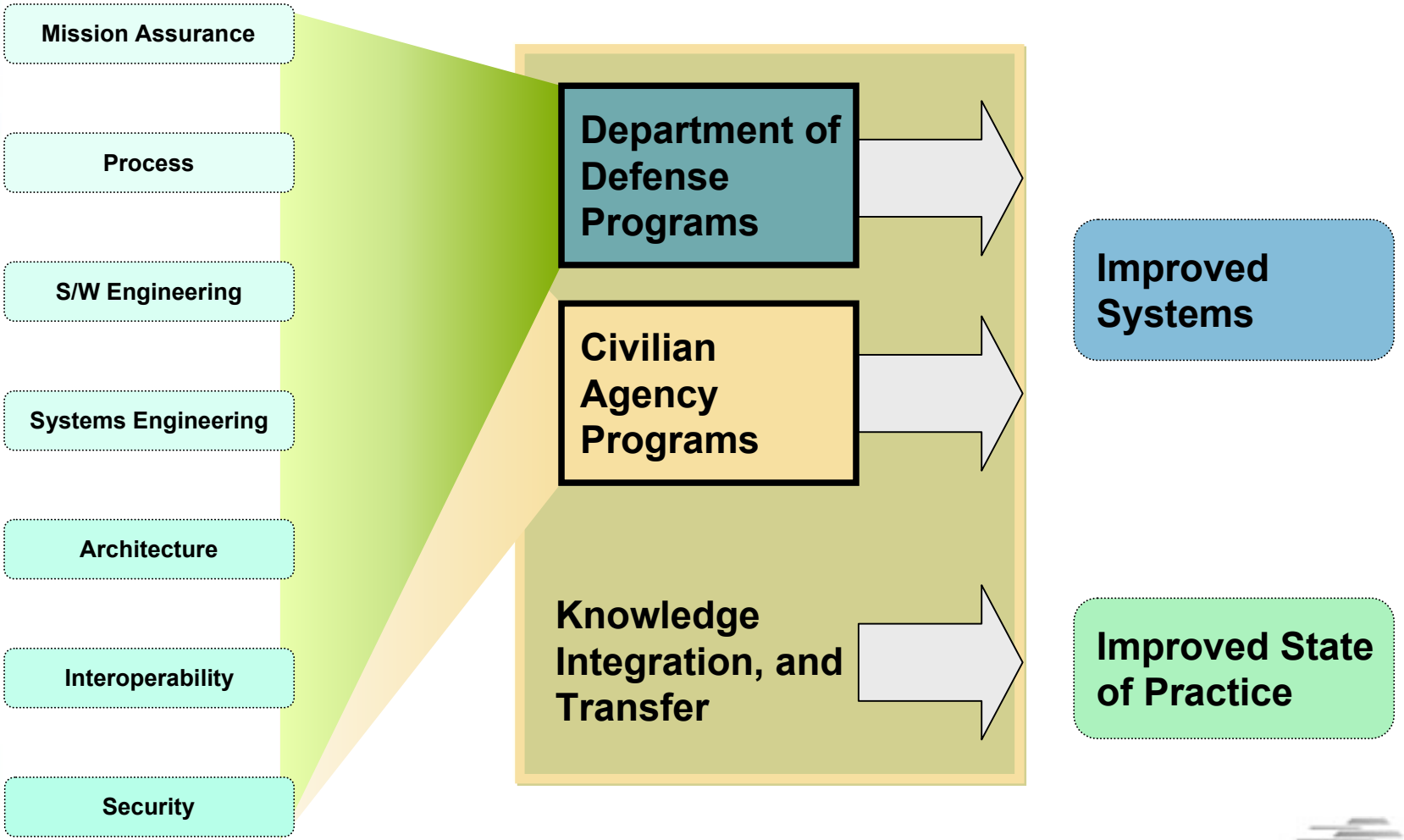
CSIRT Development Team



http://www.cert.org/csirts/

CERT

Acquisition Support Program (ASP)



CERT

Mission Assurance Team

Focused on researching and developing solutions to managing complexity.

- increasingly complex projects, programs, and processes
- multiple points of management control
- complex support technologies
- complex tasks
- multiple detailed status reports
- a variety of risks (project, security, technology, etc.), including new types of risks emerging from this complexity.

Goals of the Tutorial

Discuss the reasons, outcomes, and benefits of evaluating incident management capabilities such as CSIRTs.

Present four different methodologies that can be used to evaluate various aspects of incident management capabilities.

Provide practical exercises that demonstrate various components of each methodology to give a real-life perspective on performing such evaluations.

Evaluation Background

Evaluating Incident Management Capabilities

Once in operation, any CSIRT or similar capability will need to develop a mechanism to evaluate its operations.

This should be done in conjunction with management and the constituency.

Purpose of Evaluation

An incident management capability can be evaluated for a number of reasons, in order to

- determine if organizational functions meet requirements
- identify process improvements
  - effectiveness
  - efficiency
  - quality
- comply with standards, laws, regulations, or best practices
  - consistency
  - quality
- identify risks

Methods for Evaluation

The methods discussed in this tutorial are

- GAP analysis
  - functions
  - process
  - compliance
- Mission Assurance Analysis Protocol (MAAP)
  - process
  - function
  - risk
- CNDS Metric Assessment
  - function
  - compliance
- Mission Diagnostic Tool
  - risk

Overview of GAP Analysis

What is a GAP Analysis

"In management terms it is the space between where you are and where you want to be".

GAP Analysis is used to improve business processes.

It looks at how your organization really works, including its strength and weaknesses.

It is used to assess or compare your current operations with some set of known or best practices.

Why Use GAP Analysis?

Benchmark your organizational processes against

- another organization (center of excellence)
- a best practice
- functional compliance requirements

Identify strengths, weaknesses, and compensating factors

- process, technology, people
- interfaces and handoffs
- environmental factors
- operational considerations

Create a plan for future improvements.

However, in-depth understanding of risk is not required.

When to Use GAP Analysis

When you have

- a benchmark, baseline, or best practice to measure against
- an internal group or a third party expert team capable of performing the assessment

General GAP Analysis Process

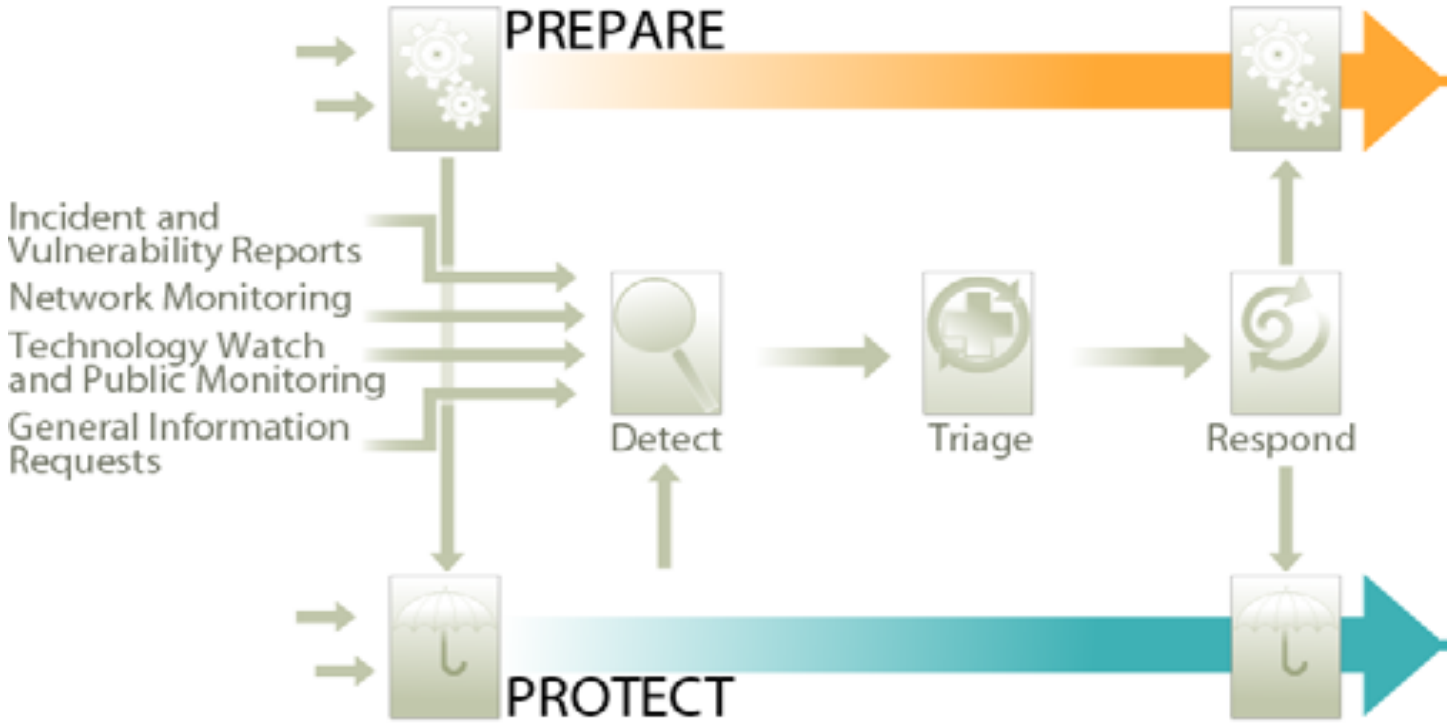
Determine benchmark or baseline for comparison.

In this case, we are using the Incident Management Process Model as a best practice baseline.

Analysis Steps:

- Define your “As-Is” or current state of incident management processes
- Perform a gap analysis of the current state
- Develop the “To-Be” or future state of your incident management processes
- Define an improvement plan that includes actions, procedures, policies, training, etc. needed to fill gaps and reach the To-Be state

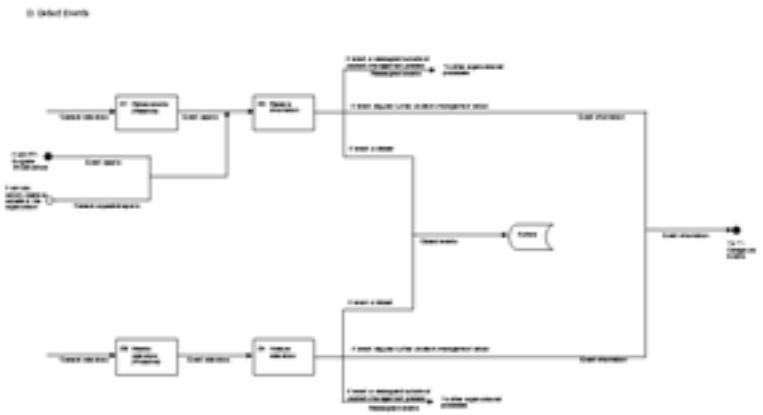
Incident Management Process Model

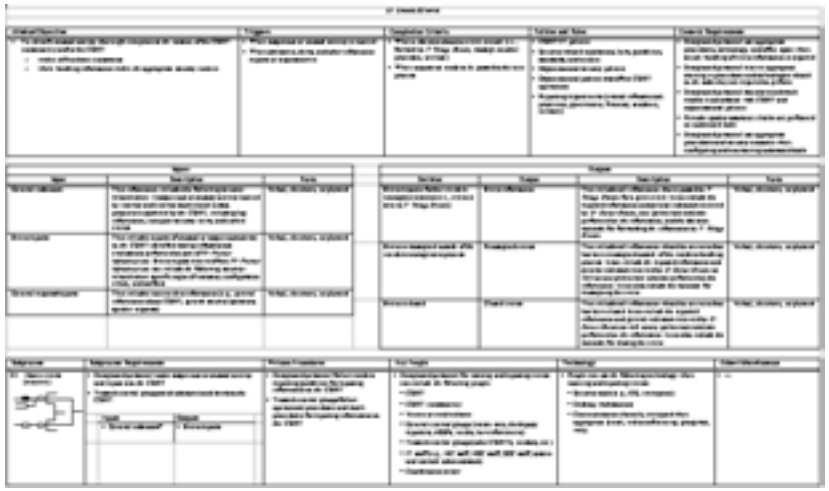


Process Model Components

The process model is comprised of

- Process Workflows
- Workflow Descriptions



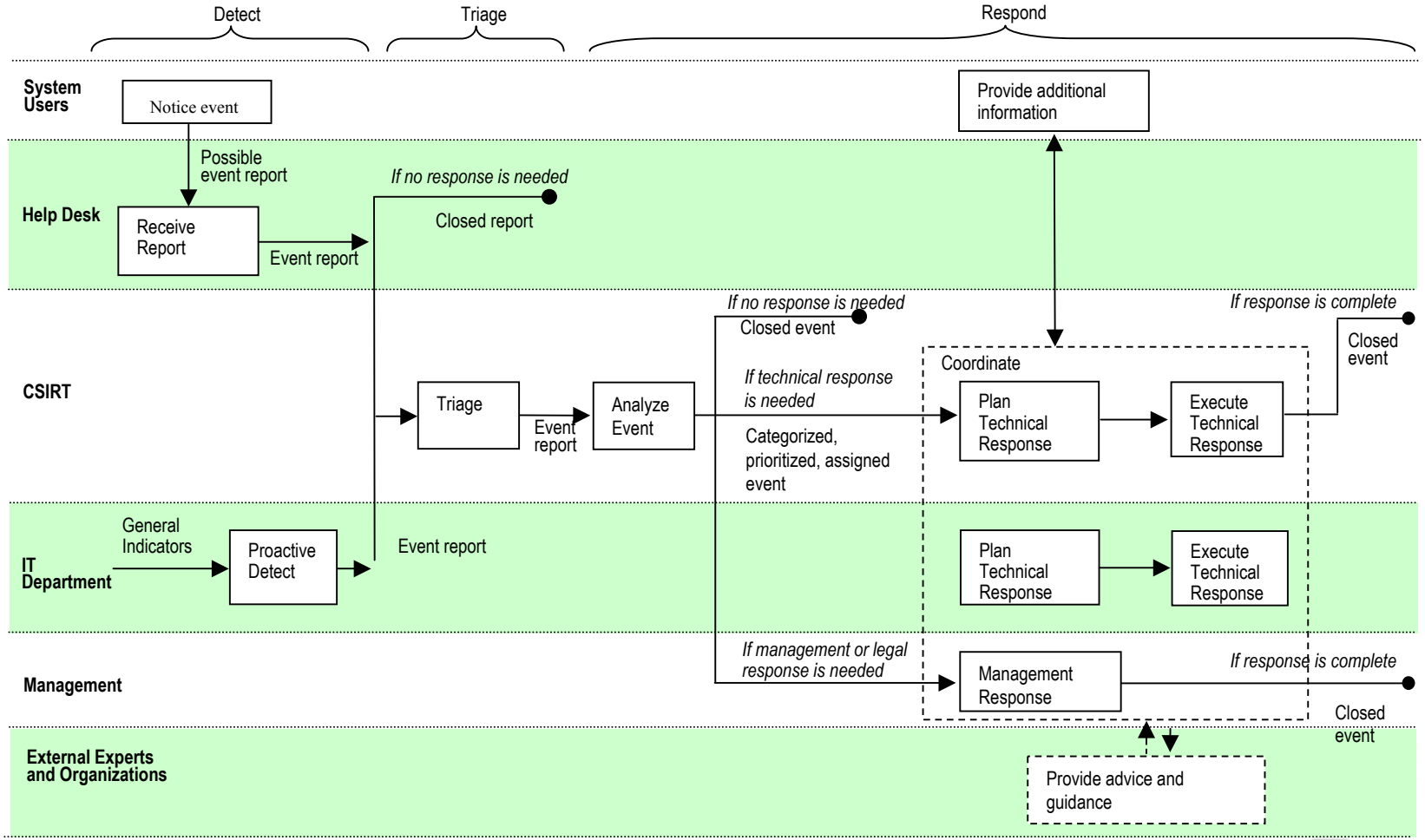


Build the As-Is

Build the As-Is process map using the incident management process model as guidance

- gather data through interviews, documentation review, or observation
- redline or modify the process model workflows and descriptions
- add any relevant local processes, activities, or interfaces
- revise process descriptions for each process, activity, and interface
- review and finalize

Resulting Swimlane Diagram



Perform Gap Analysis

Compare your As-Is state against the Process Model.

Perform a traditional gap analysis by looking for characteristics such as

- missing or poorly defined handoffs
- missing or poorly defined aspects of each process activity (e.g., no procedures or inadequate staff)
- bottlenecks in the process
- poorly defined activity flows (e.g., too much parallelism, too linear, too many handoffs)
- single points of failure

Build the To-Be State

Build the To-Be process map by modifying the As-Is

- identify new activities
- identify improvements to poor characteristics such missing procedures or poorly trained staff
- streamline inefficient flows
- redesign bottlenecks
- establish missing interfaces

Build the Improvement Plan

Use the To-Be process as

- **the goal of an improvement plan**
- **guidance for implementing the plan**

Take steps to

- establish a project team, if appropriate
- establish a roll-out plan
- set up communications channels
- prioritize and schedule changes, such as
  - build missing procedures
  - acquire needed training
  - add personnel
  - revise contracts for improved handoffs
- monitor progress and watch for unintended consequences (e.g., unexpected bottlenecks)
- document lessons learned
- re-evaluate the revised process

Exercise: Analyze To-Be State

Overview of Mission Assurance Analysis Protocol

Key Aspects of Mission Assurance

Key aspects of mission assurance include

- dual focus on outcome and execution
- portfolio view of mission risk
- measure of mission risk

Mission risk is defined as the possibility that a mission might not be successfully achieved.

- product/outcome risk
- process risk
- people risk
- technology risk
- security risk
- interoperability risk
- business environment risk
- event risk
- change risk
- other risks

Establishing Mission Assurance

Establishing a reasonable degree of confidence in mission success for an incident management process requires considering the following perspectives:

- local
- organizational
- inter-organizational

What is MAAP?

MAAP is a protocol, or heuristic, for determining the mission assurance of an incident management process.

MAAP

- applies an engineering approach to risk analysis
- designed for highly complex environments (multi-organization, system of systems)
- provides an in-depth analysis of processes, relationships, and dependencies
- characterizes the risk of operational failures
  - process performance risk
  - security risk
  - operational environment risk

Why Use MAAP?

To acquire an in-depth view of mission risk.

- Mission failure has an unacceptable cost to the organization.
- Mission failure has disastrous consequences to customers, constituents, or other people.

Current risk analysis techniques are too limited

- do not account for risk that is inherited from previously completed activities
- consider a limited number of risk sources (e.g., only security risks are analyzed)
- cannot characterize risk arising from the interrelationships and dependencies found in distributed processes

When to Use MAAP

You have sufficient risk management expertise and general process analysis skills to identify and analyze complex risks.

You have stable work processes that can be documented and analyzed.

You have complex work processes that cross multiple working groups or organizations.

Managing Complexity

Managers are becoming responsible for overseeing increasingly complex projects, programs, and processes.

- multiple points of management control
- complex support technologies
- complex tasks
- multiple detailed status reports
- a variety of risk management data (project, security, technology, etc.)

New types of risks have emerged from this complexity.

General MAAP Process

Acquire an in-depth view of mission risk.

Based on work flow processes and complex risk analysis.

MAAP Steps:

- Begin with As-Is work process flow.
- Evaluate risk at each transition point.
- Evaluate end-to-end risk to mission.
- Create risk “cause-and-effect” diagrams and look for root. causes, chains, aggravating and mitigating conditions.
- Prioritize risks based on impact to mission.
- Mitigate risks in the To-Be work process, with revised policies, procedures, training, technology, etc.

General MAAP Process

Begin with As-Is work process flow.

Evaluate risk at each transition point.

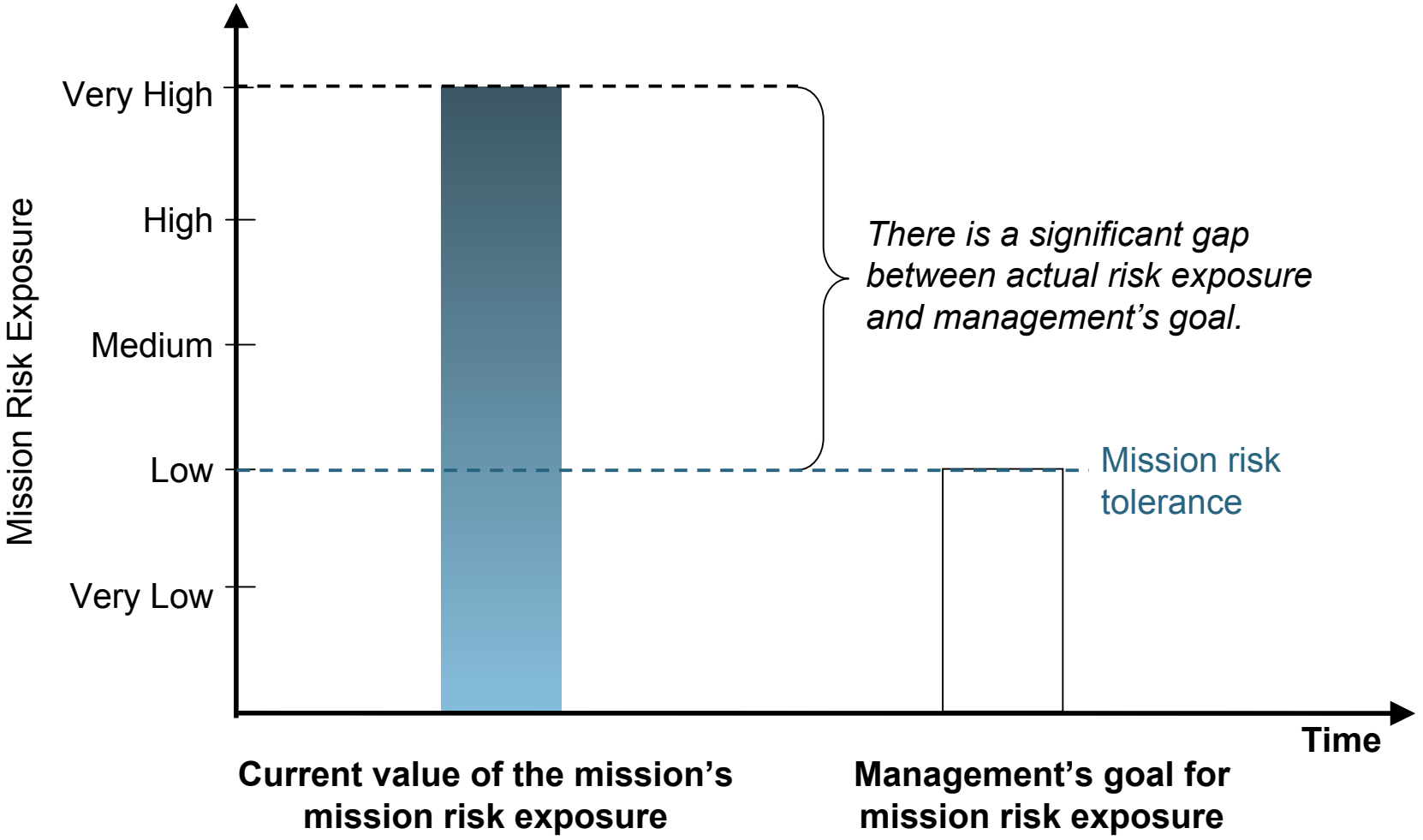
Evaluate end-to-end risk to mission.

If possible, create risk “cause-and-effect” diagrams and look for root causes, chains, aggravating and mitigating conditions.

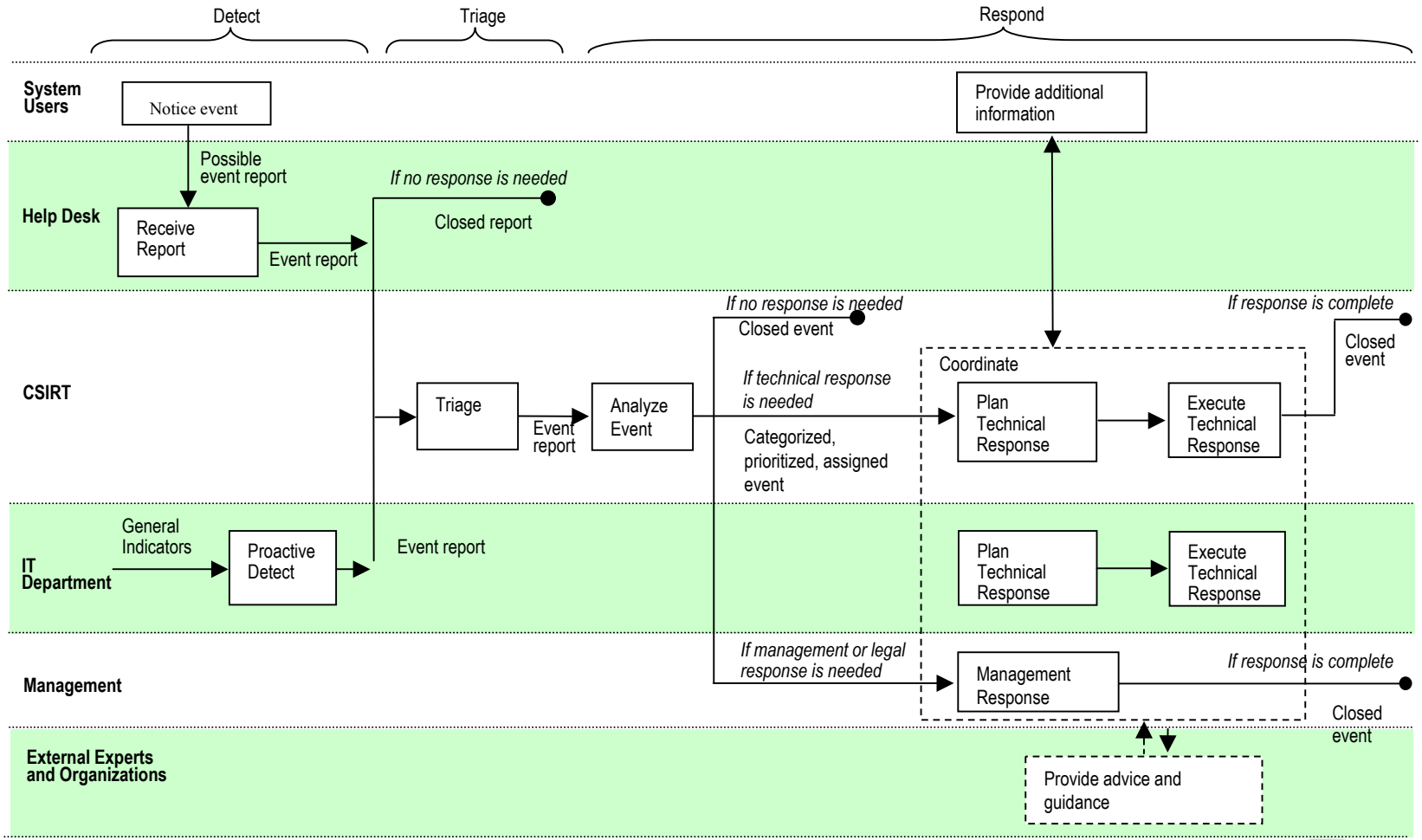
Prioritize risks based on impact to mission.

Mitigate risks with a To-Be work process and revised policies, procedures, training, etc.

Bringing Risk within Tolerance

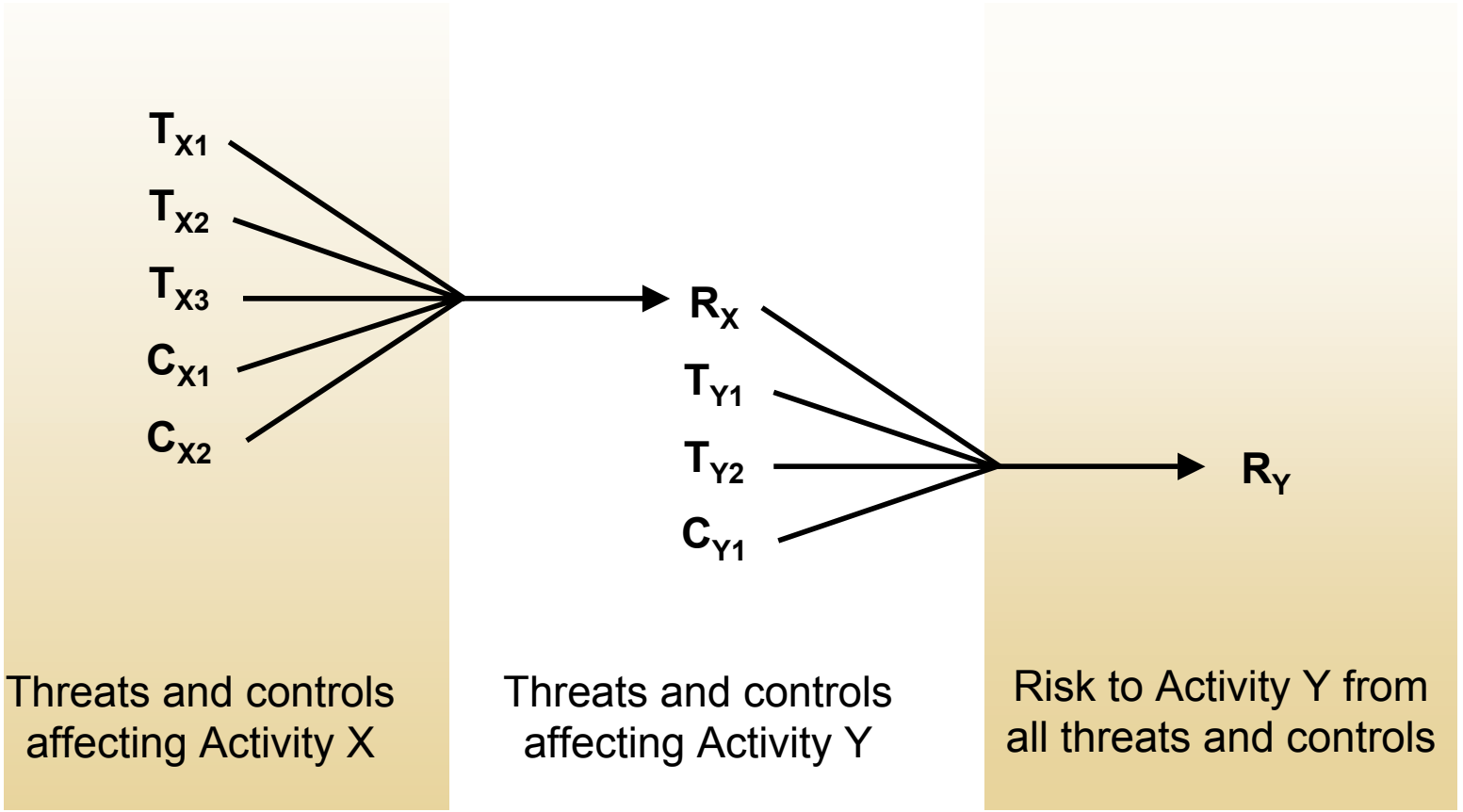


Remember the Process Workflow

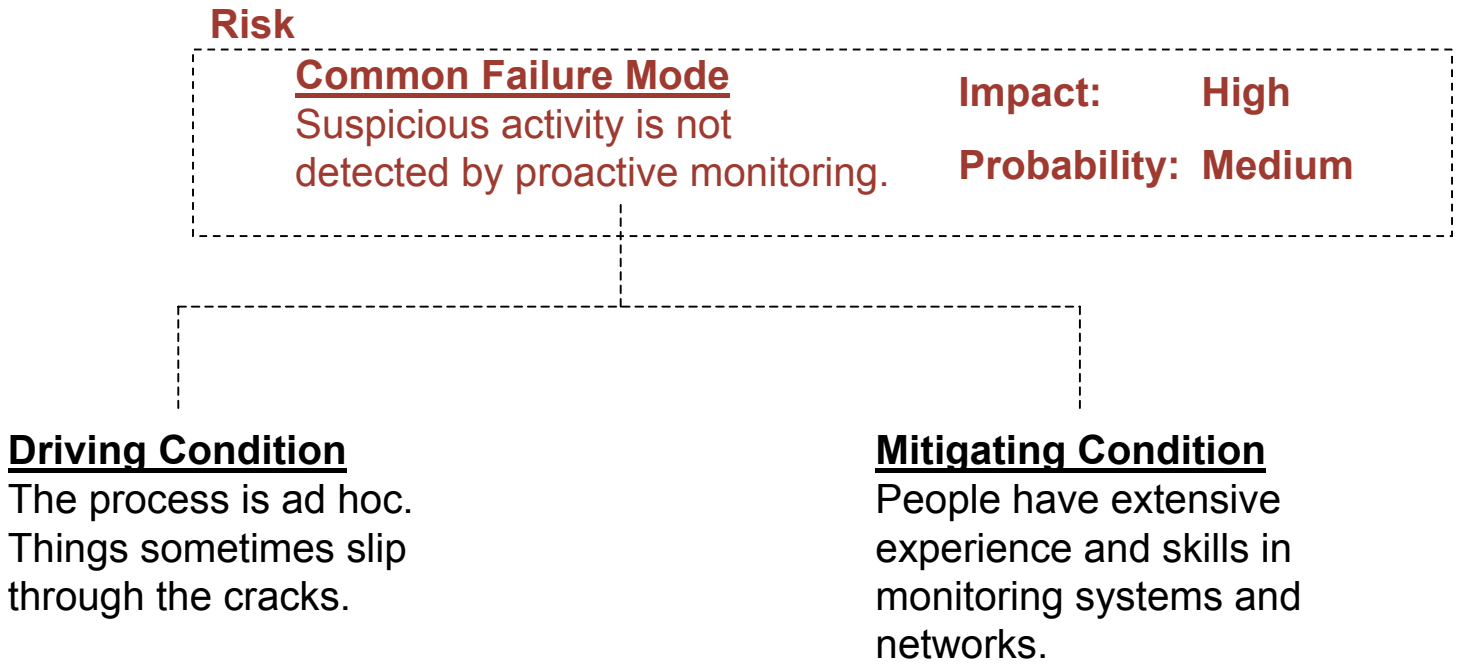


Analyzing Multiple States

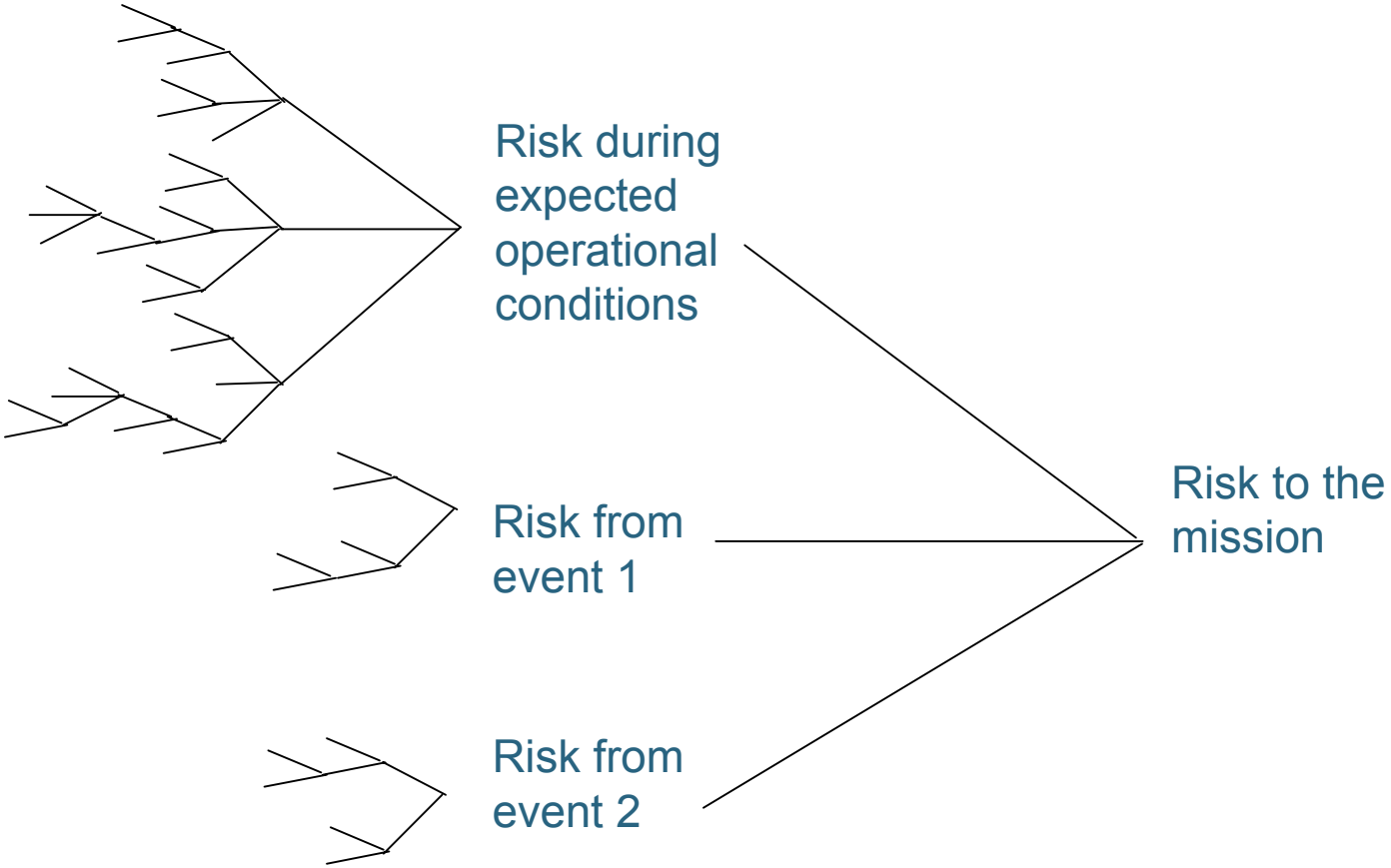
Interrelated View of Risks



Example: Influencing Conditions

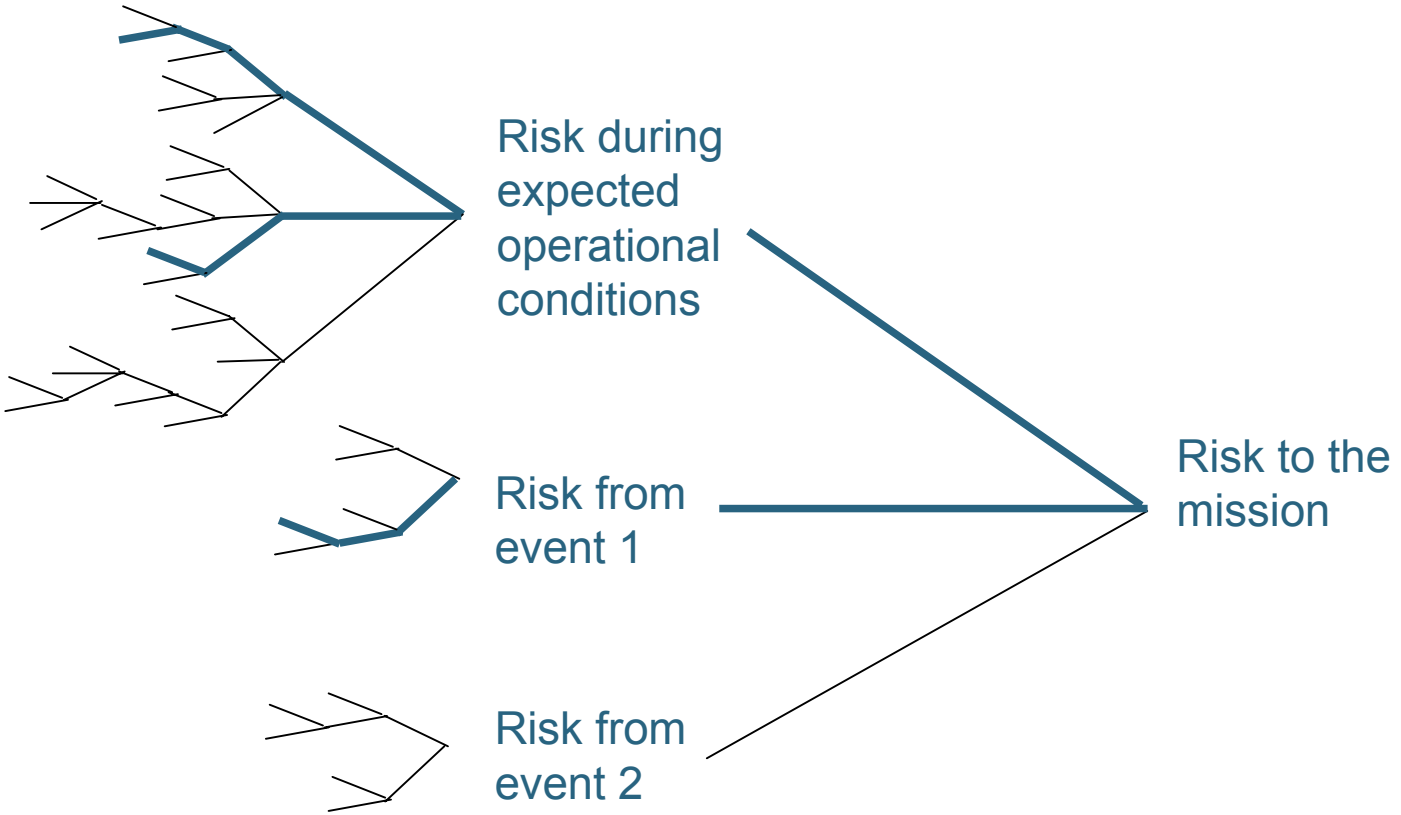


Risk Causal Chain



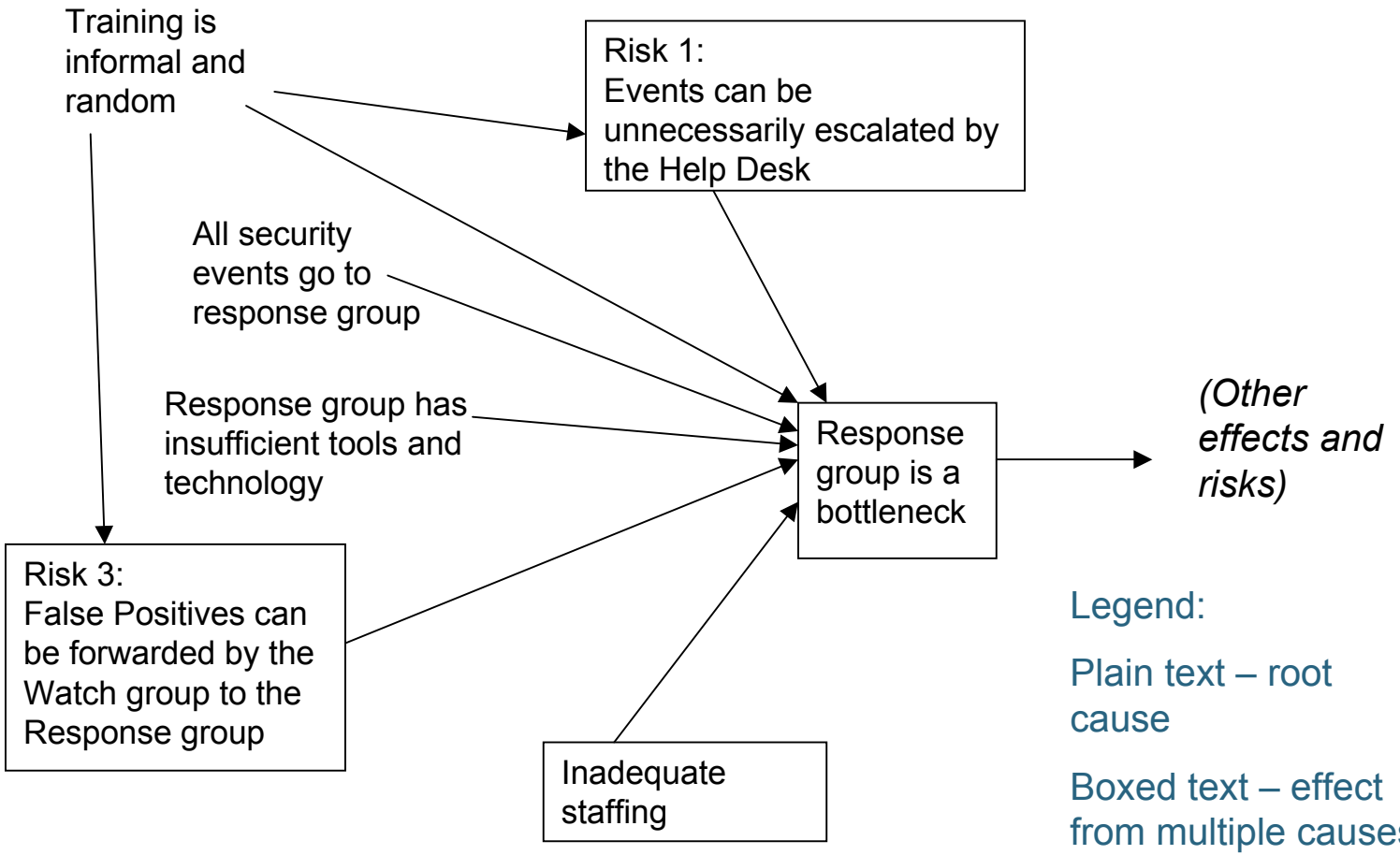
Combinations of threats, vulnerabilities and controls → **Risk resulting from different operational circumstances** → **Mission risk**

Key Risk Drivers



A critical path analysis identifies the key risk drivers.

Example: Complex Risks (Partial)



Exercise: Analyze Complex Risks

Overview of CND Metrics Assessment

CND Metrics

US-CERT is currently sponsoring the development of Computer Network Defense (CND) evaluation metrics for federal, state, and local government agencies.

- Adapted from the DoD 8530 Directive and Instruction.

Pilot testing of metrics and assessment process are underway.

A more general version of these metrics is planned for release and use by teams and organizations as a self-assessment tool.

This is a preview of that effort.

Original DoD CNDSP Metrics

DoD 8530 Directive and Instruction provides guidance to

- evaluate Computer Network Defense Service Providers (CNDSP)
- certify and accredit teams

Secondary goal: ensure a higher quality of protection through increased maturity and understanding of the services provided by the CNDSP.

Goals of the CND Metrics

Provide organizations with an assessment tool that can be used to benchmark their incident management capability.

Assist organizations in identifying any areas for improvement in the Protect, Detect, Respond, and Sustain functions for Computer Network Defense (CND).

Why Use the Metrics Assessment

You want to know if you have all the basic components required for an incident management capability.

You want to know if your service provider has sufficient components to provide the capability under contract.

You need to know how to relate incident management functions to regulations.

You do not need an in-depth understanding of mission risk.

When to Use the Metrics Assessment

You have a group of people who can use these metrics to self-assess and they can be completely honest about their own strengths and weaknesses.

OR

You can find an expert team to assess your incident management capability and provide an independent viewpoint.

Metrics Categories and Priorities

Divided into four major service categories:

- Protect
- Detect
- Response
- Sustainment

Priority I metrics = critical services for an incident management capability.

Priority II metrics = next most important services; address traditional operational concerns.

Priority III and Priority IV metrics = best practices that support operational effectiveness and quality.

Metric Service Categories

Protect	Detect	Response	Sustainment
Risk Assessment Support	Network Security Monitoring	Incident Reporting	MOUs and Contracts
Vulnerability Assessment Support	Indicators, Warning, and Situational Awareness	Incident Response	Project/Program Management
Virus/Malware Protection Support		Incident Analysis	CND Technology Development, Evaluation and Implementation
CND Operational Exercises			Personnel
Constituent Protection Support and Training			Security Administration
Information Assurance/ Vulnerability Management			CND Information Systems

Scoring the Metrics

Not Applicable (NA)	The metric did not apply to the organization; excluded from a total “score”.
Not Observed	The metric was not observed during the interview
Yes	The metric was met.
Partial	The metric was partially met.
No	The metric was not met.

CND Metrics				
3.1.4	**Metrics question?**		**Priority I**	
Not observed	Not applicable	**Metrics statement.**	Y	N
Prerequisites ….. [R] **Control** ….. [R] …… **Activity** …. [R] …. **Supporting Mechanisms** …. [R] …. **Artifacts** …. [R] …. **Quality** … [R] ….				
DoD CNDSP Metric Reference(s):				
Regulatory References:				
Guidance References:				
Organization References:				

Metrics Indicators

Each metric contains a set of “indicators”

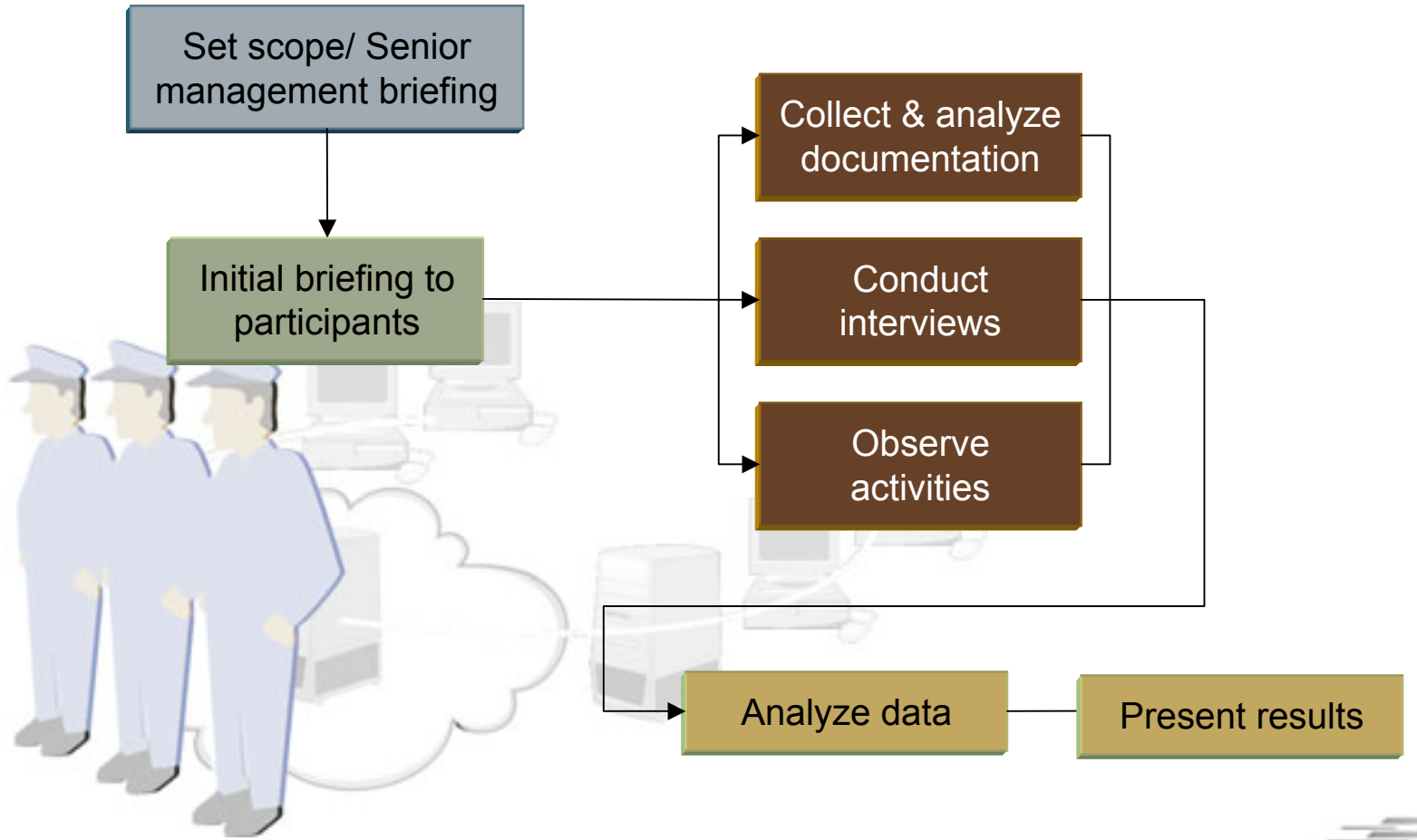
- pre-requisites that are needed
- controls that are available or exist
- activities that are performed
- supporting mechanisms
- artifacts that can be observed or demonstrated
- quality mechanisms that establish effective, quality service provision

Metrics Guidance

Supports the use of metrics as self-assessment tool.

Provides the evaluators with additional information to help them determine whether or not the indicators and the metric have been met.

Expert Team CND Assessment Process



Conduct Interviews

Gather metrics information.

- Use metrics relevant to participants.
- Identify additional documentation that should be gathered and reviewed.
- Identify any activities that should be observed.

Metrics Analysis

Evaluators analyze data collected during interviews (or self assessment) to

- validate whether the organization meets the required indicators of the metric (designated by items with a bracketed [R])
- make a qualified judgment as to whether or not the metric has successfully been satisfied
- determine the quality of the performance of that metric (where possible)

Building the Improvement Plan

Fix the Priority I metrics that you did not meet.

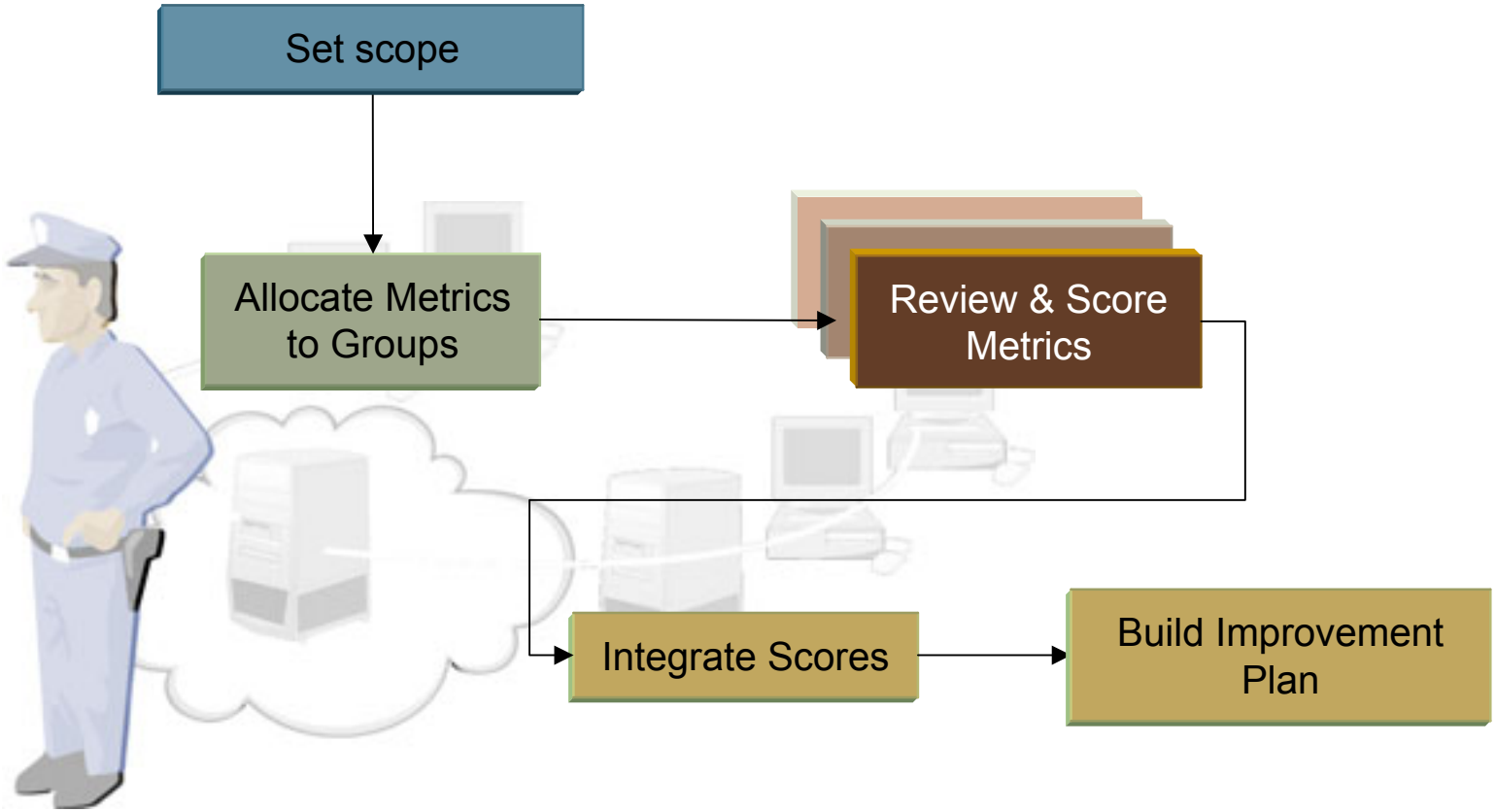
Fix the Priority II metrics that you partially met.

Work through the rest of the Priority II, III, and IV metrics

- Focus on the metrics you partially met.
- Start improving the metrics you did not meet to gain at least partial improvement.

Consider the common threads in the metrics you did not meet, such as missing documentation or inadequate training.

Self-Directed CND Assessment



Self-Directed CND Assessment

Set scope of assessment.

- what functions will be included?
- which groups will be included?

Allocate metrics to each group.

Each group reviews the metrics and scores themselves.

Collect all the metrics scores and consolidate results.

Build the improvement plan.

Exercise: Evaluate One Metric

Overview of the Mission Diagnostic

Exercise: Abbreviated Mission Diagnostic (Part 1)

What is the Mission Diagnostic?

Designed to complement assessments with no risk component.

Can be used to estimate the risk to an agency's incident management mission as part of a

- CND metrics assessment
- Gap Analysis

Developed as part of SEI's Mission Assurance project.

- Provides a relatively rapid evaluation of a mission's overall risk exposure.
- Uses ten common risk indicators are used to estimate a mission's overall risk exposure.

Why Use the Mission Diagnostic?

You need something quick to estimate mission risk exposure.

You only want a general indication of how well mission objectives are being met. You don't need

- a detailed measure of risk
- to identify all root causes of risk

You are already doing a complex, time-consuming evaluation and do not have the resources for a full-blown risk assessment.

When to Use Mission Diagnostic

You have only a small amount of risk expertise and experience.

You need a risk viewpoint but don't have the time or resources for an complete risk assessment.

You are already doing another type of assessment that has no risk element.

Risk Indicators Examined

- Unrealistic or unarticulated goals
- Poor communication
- Customer requirements and needs not well understood
- Stakeholder politics or other external pressures
- Inefficient or ineffective process
- Lack of process control
- Poor task execution
- Insufficient staffing
- Inadequate technological and infrastructure support
- Inability to manage changing circumstances or unpredictable events

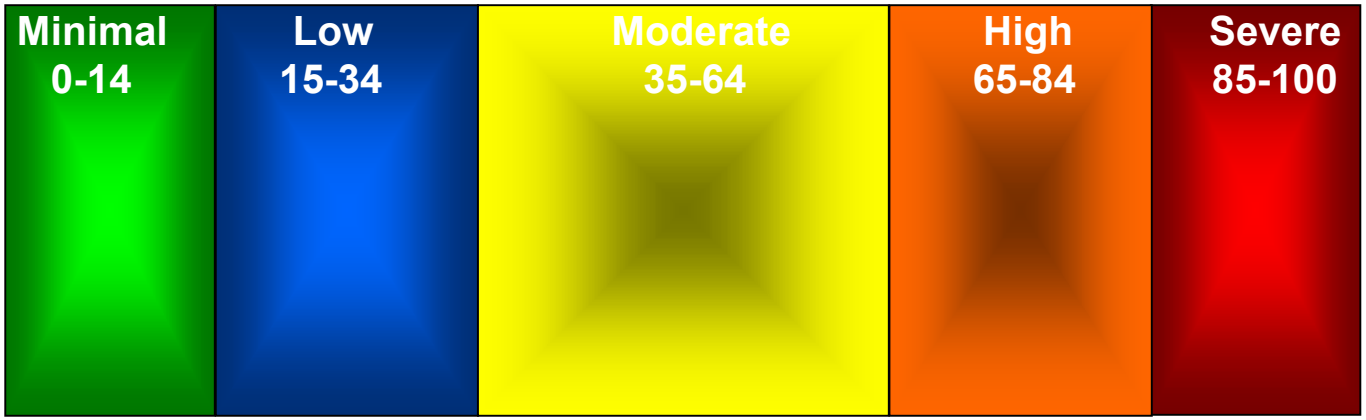
Scoring an Indicator

	Indicator	To what extent is this statement true for your incident management capability?
		Not At All — Somewhat — Very Much
1	Unrealistic or unarticulated goals	|----------|----------|----------X----------|
		0 2.5 5 7.5 10

The ‘X’ on the scale is based on the collective judgment of evaluation team about the presence or absence of the indicator in this organization.

The score for this example indicator is 7.5 – unrealistic or unarticulated goals are common.

Estimating the Risk Exposure



A total risk score is determined by adding the scores for all individual statements (10 indicators, 10 possible points each).

The risk exposure is determined by comparing total risk score to the simple scale above.

Example: Indicator Scores

Unrealistic or unarticulated goals – 5.0

Poor communication – 5.0

Customer requirements and needs not well understood – 0

Stakeholder politics or other external pressures – 2.5

Inefficient or ineffective process – 2.5

Lack of process control – 5.0

Poor task execution – 2.5

Insufficient staffing – 7.5

Inadequate technological and infrastructure support – 2.5

Inability to manage changing circumstances or unpredictable events – 2.5

TOTAL = 35, or Moderate Risk

Exercise: Abbreviated Mission Diagnostic (Part 2)

Summary

Evaluation Method	Purpose?	Why?	When?
GAP Analysis			
MAAP			
CND Metrics			
Mission Diagnostic			

Contact Information

Mission Assurance Team
Acquisitions Support Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

Web:

http://www.sei.cmu.edu/programs/acquisition-support/

Email:

Audrey Dorofee
ajd@sei.cmu.edu

Christopher Alberts
cja@sei.cmu.edu

CERT CSIRT Development Team
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

Web: http://www.cert.org/csirts/

Email: csirt-info@cert.org

Robin Ruefle
rmr@cert.org