

# U.S. Army Training and Doctrine Command Mad Scientist Series – Intelligence Preparation for Operational Resilience (IPOR)

Douglas Gray

29 June 2016

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213



Software Engineering Institute

Carnegie Mellon University

© 2016 Carnegie Mellon University

Distribution Statement A: Approved for Public Release;  
Distribution is Unlimited

# Notices

Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

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 may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon®, CERT® and OCTAVE® are registered marks of Carnegie Mellon University.

Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup>

DM-0003754

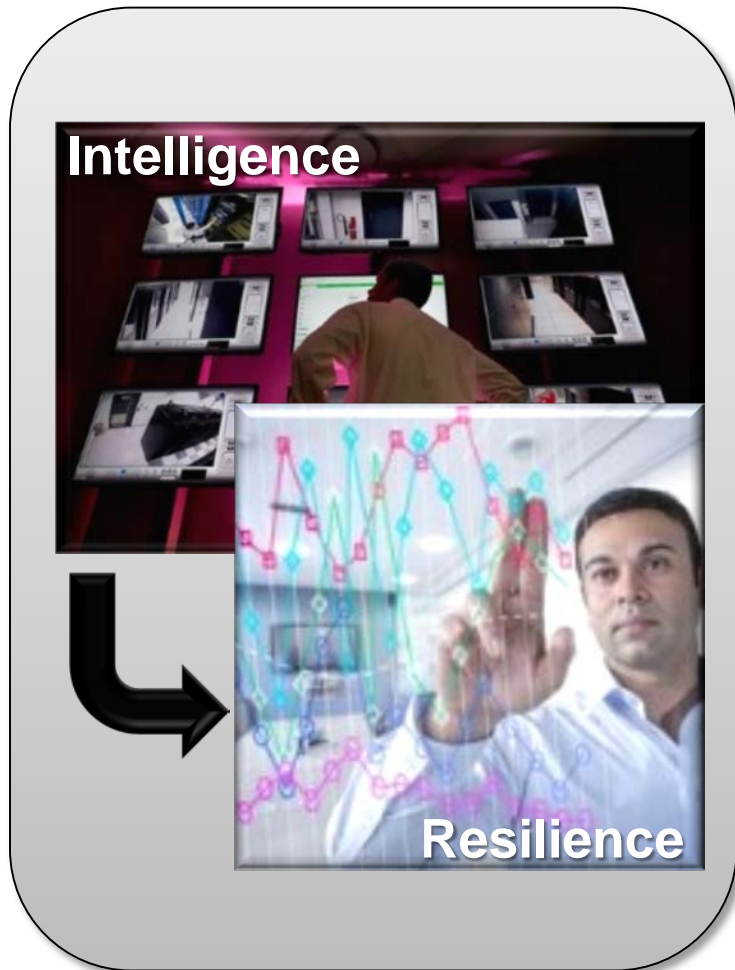


Intelligence Preparation for Operational  
Resilience (IPOR)

# Introduction



# Opportunities to Extend IPB



Intelligence Preparation of the Battlefield (IPB) enables Army organizations to

- enable understanding of threat, environment and options for friendly and enemy forces
- determine
  - what information they need
  - what information they have
  - what information they must obtain
- integrate information to develop situational awareness

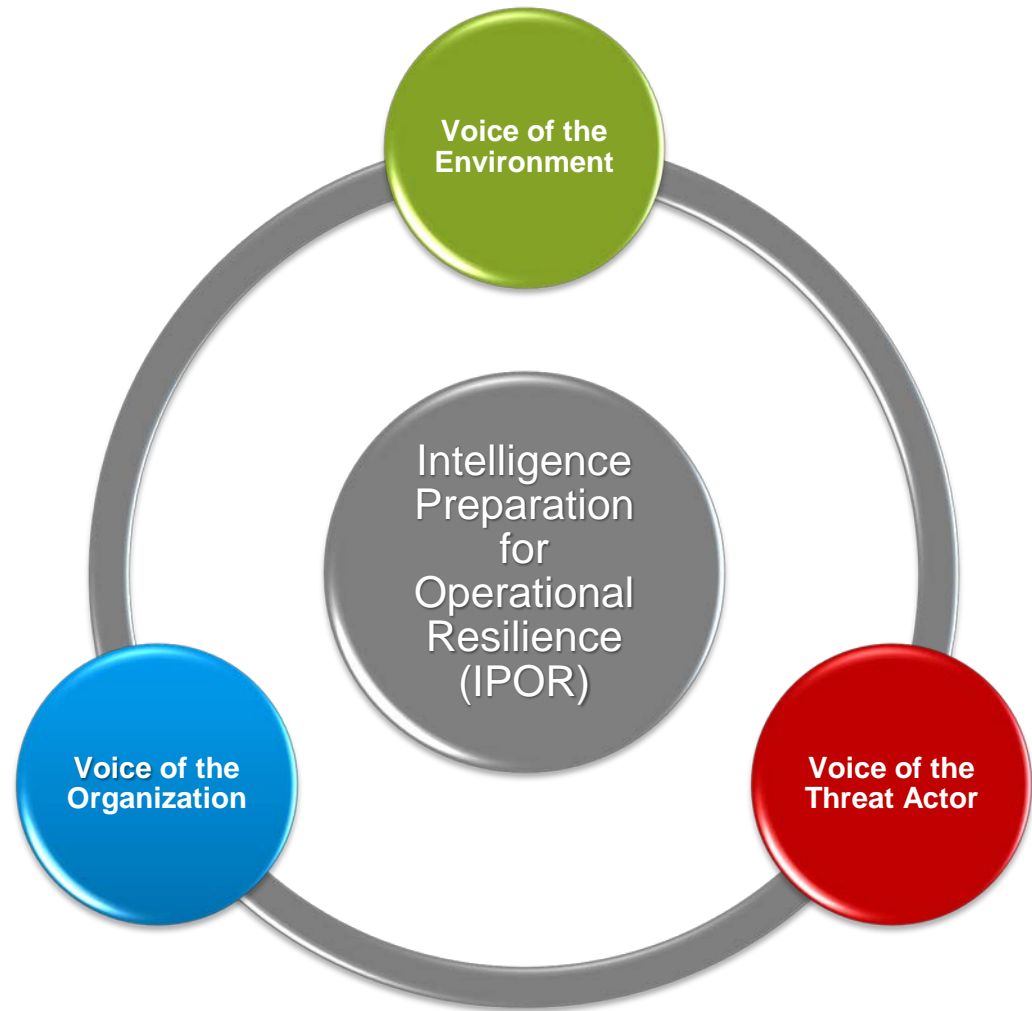
Opportunities:

- create common framework for non-DOD organizations (inter-agency, private sector)
- opportunity for more focus on operational resilience/cybersecurity context-setting
- opportunity to tie directly into risk management

# What is IPOR?

IPB re-organized to

- be accessible to non-DOD, enhance inter-agency and public/private sector information sharing
- leverage established resilience management model
- tie directly in with risk-management and project-management frameworks



# Leveraging Existing Frameworks

IPOR integrates, leverages and/or builds upon existing frameworks, such as...

- Intelligence Preparation of the Battlefield (IPB) process
- CERT® Resilience Management Model (CERT-RMM)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro
- National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)
- Agile
- Project Management Body of Knowledge

# Threat Actors, Threats, Risks

## Threat Actor

- “a situation, entity, individual, group, or action that has the potential to exploit a threat”

## Threat

- “combination of a vulnerability, a threat actor, a motive (if the threat actor is a person or persons), and the potential to produce a harmful outcome for the organization”

## Risk

- “combination of a threat and a vulnerability (condition), the impact (consequence) on the organization if the vulnerability is exploited, and the presence of uncertainty”

# Operational Resilience

**The ability of the organization to achieve its mission even under degraded circumstances**

## **Resilient Services – Able to Support the Strategic Objectives**

- Maneuver
- Fires and effects
- Combat service support (CSS)
- Civil military operations (CMO)
- Command, control, computers, intelligence, surveillance, reconnaissance (C4ISR)

## **Resilient Assets – Able to Support Services**

- People
- Information
- Technology
- Facilities
- Supply chain/raw materials (e.g., vendors, cloud)

# Building Situational Awareness

## Levels of Situation Awareness

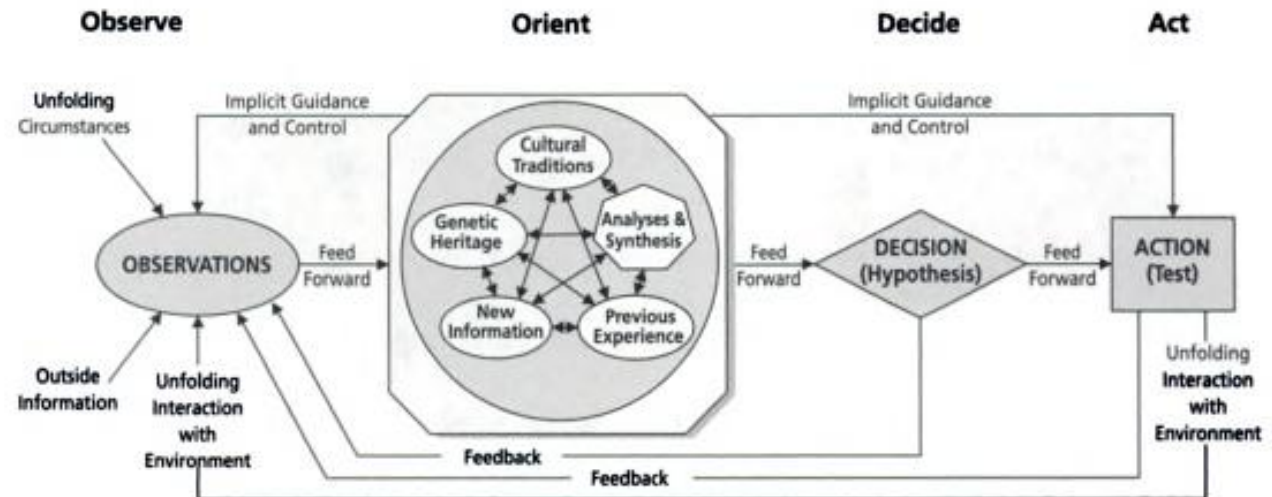
**Level 1**  
perception of  
the elements in  
the environment

**Level 2**  
comprehension  
of the current  
situation

**Level 3**  
projection of  
future status

[Endsley 2012, p. 14]

## Boyd's OODA Loop



Note how ORIENTATION shapes OBSERVATION, shapes DECISION, shapes ACTION, and in turn is shaped by the feedback and other phenomena coming into our sensing or observing window.

Also note how the entire "loop" (not just ORIENTATION) is an ongoing, many-sided implicit cross-referencing process of projection, empathy, correlation, and rejection.

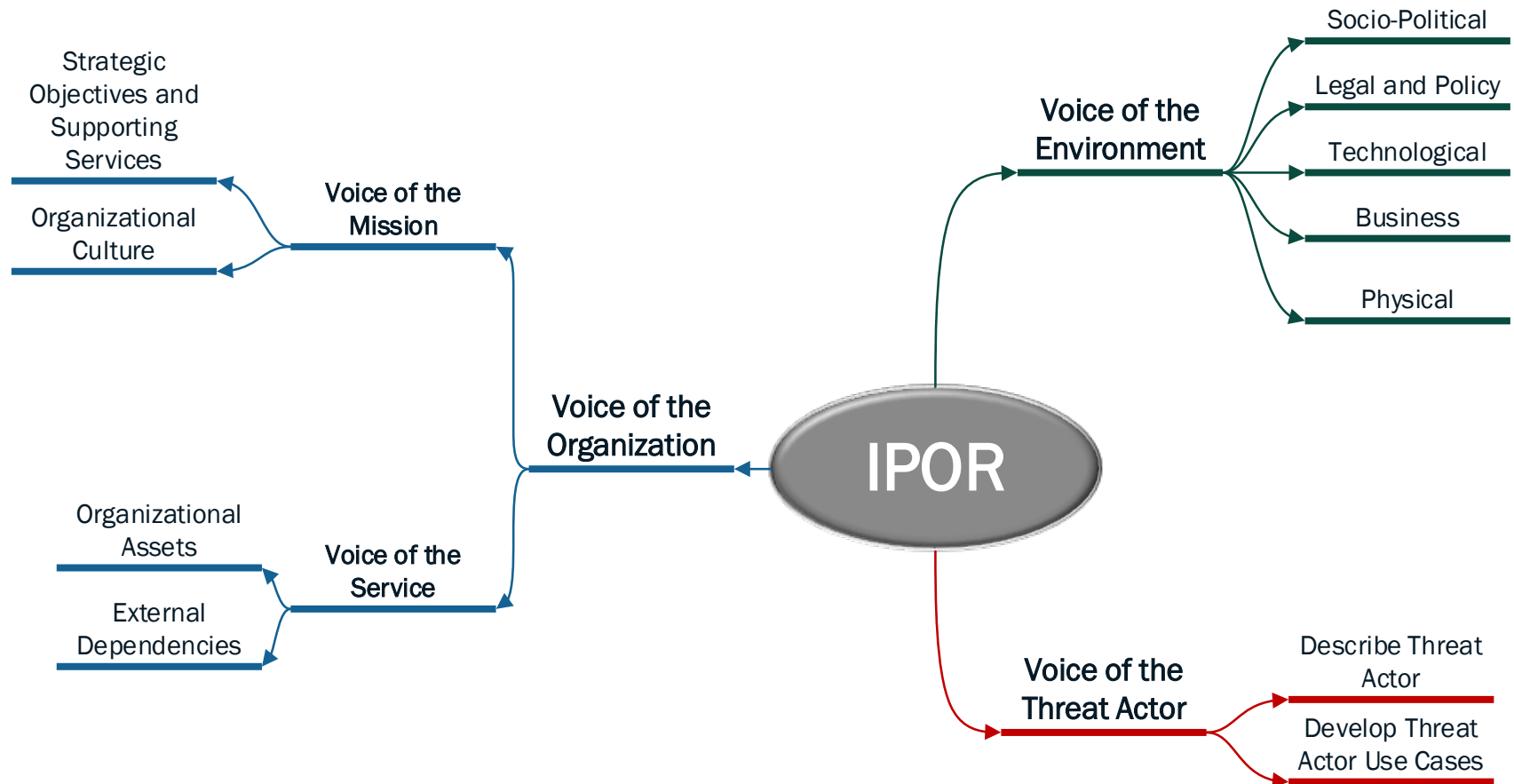
John R. Boyd, 1992

Intelligence Preparation for Operational  
Resilience

# IPOR Overview



# Decomposing Information



# Voice of the Environment

## Determine the Socio-Political Environment

- Nation state conflicts
- Nation state cooperation
- Political perception of company

## Determine the Legal and Policy Environment

- Statutes, treaties (pending and on the books)
- Court cases
- Insurance coverage

## Determine the Technological Environment

- Cloud, mobile, etc.
- Encryption

## Determine the Business Environment

- Effects of consumer and shareholder confidence
- Effects of operational resilience on brand image

## Determine the Physical Environment

- Natural hazards (prone to hurricanes, tornados, earthquakes)
- Positioning of and access to facilities

# Voice of the Organization

## Voice of the Mission

- Organizational context
- Strategic Objectives
- High-value services
- Organizational culture

## Voice of the Service

- Organizational assets that support high-value services
  - People
  - Information
  - Technology
  - Facilities
- External dependencies
  - Vendors, partners
  - Externally managed assets (i.e., cloud)

# Voice of the Threat Actor

## Develop Threat Actor Taxonomy

- NIST RMF categories
  - Hostile cyber/physical attacks
  - Human errors of omission or commission
  - Natural and man-made disasters
- Intel Threat Agent Library
- Customize to organizational needs
- Support Information sharing

## Develop Threat Use Cases

- Service(s)/asset(s) threatened
- Potentially interested threat actor categories
- Intentions
- Motivations
- Most likely attack pattern
- Evidence/historical information?

Intelligence Preparation for Operational  
Resilience (IPOR)

# Operationalizing Intelligence



Software Engineering Institute

Carnegie Mellon University

© 2015 Carnegie Mellon University

Distribution Statement A: Approved for Public Release;  
Distribution is Unlimited

# Operationalizing IPOR



# Use of Risk, Resilience, and Project Management Frameworks

## Risk and Resilience Management

- CERT® Resilience Management Model (CERT-RMM)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro
- NIST Risk Management Framework

## Project Management

- Agile
- Project Management Body of Knowledge (PMBOK)

# What is CERT-RMM?

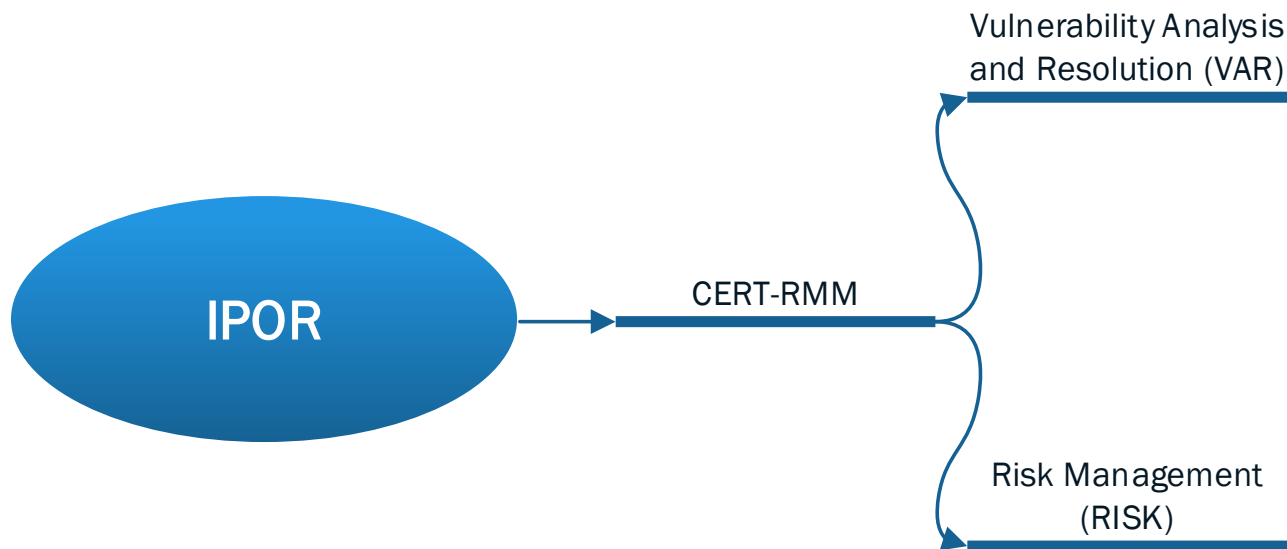
*CERT-RMM is a capability model for managing and improving operational resilience.*

***“...an extensive super-set of the things an organization could do to be more resilient.”***

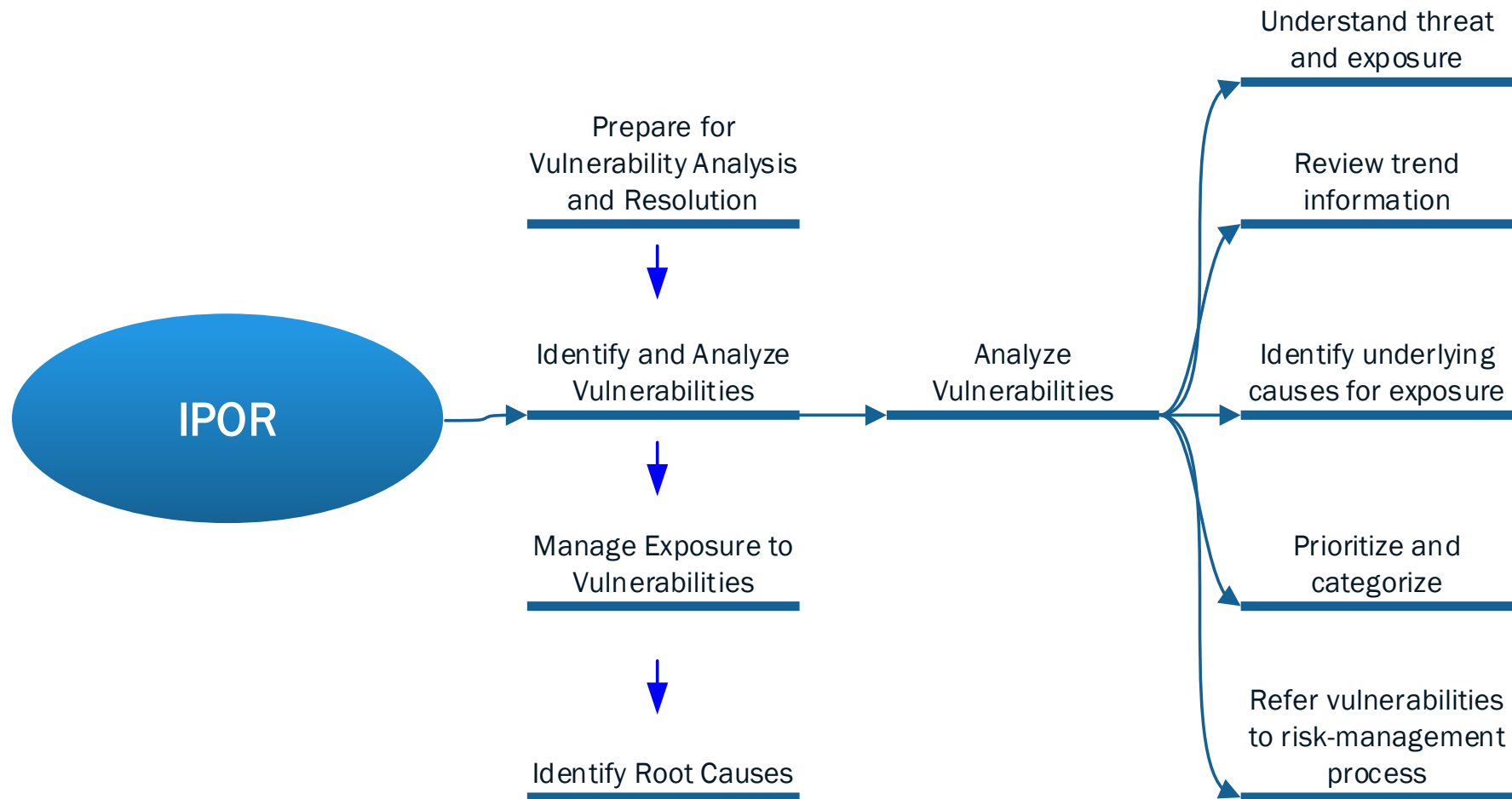
*- CERT-RMM adopter*

- **Guides implementation and management of operational resilience activities**
- **Converges key operational risk management activities: security, BC/DR, and IT operations**
- **Defines maturity through capability levels**
- **Enables measurement**
- **Improves confidence in how an organization responds in times of operational stress**

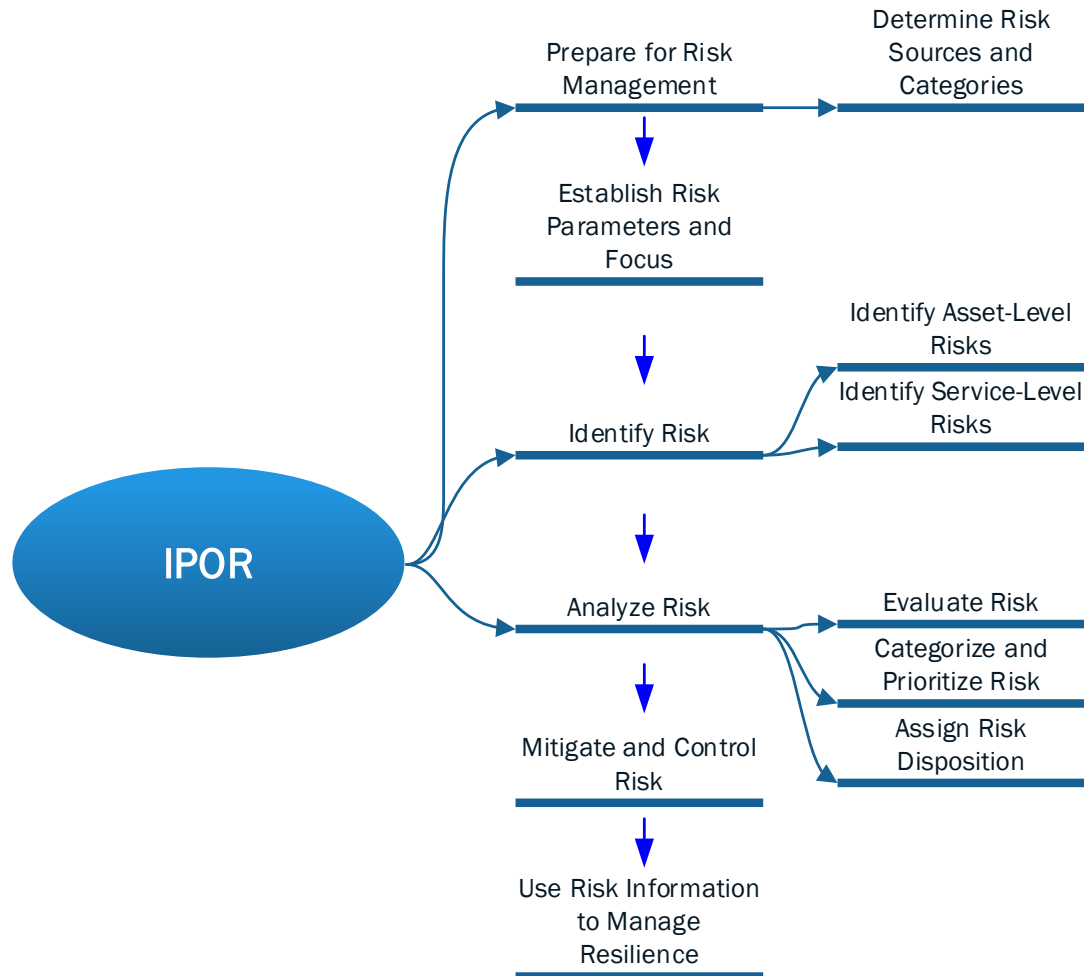
# Leveraging Threat Intelligence in CERT-RMM



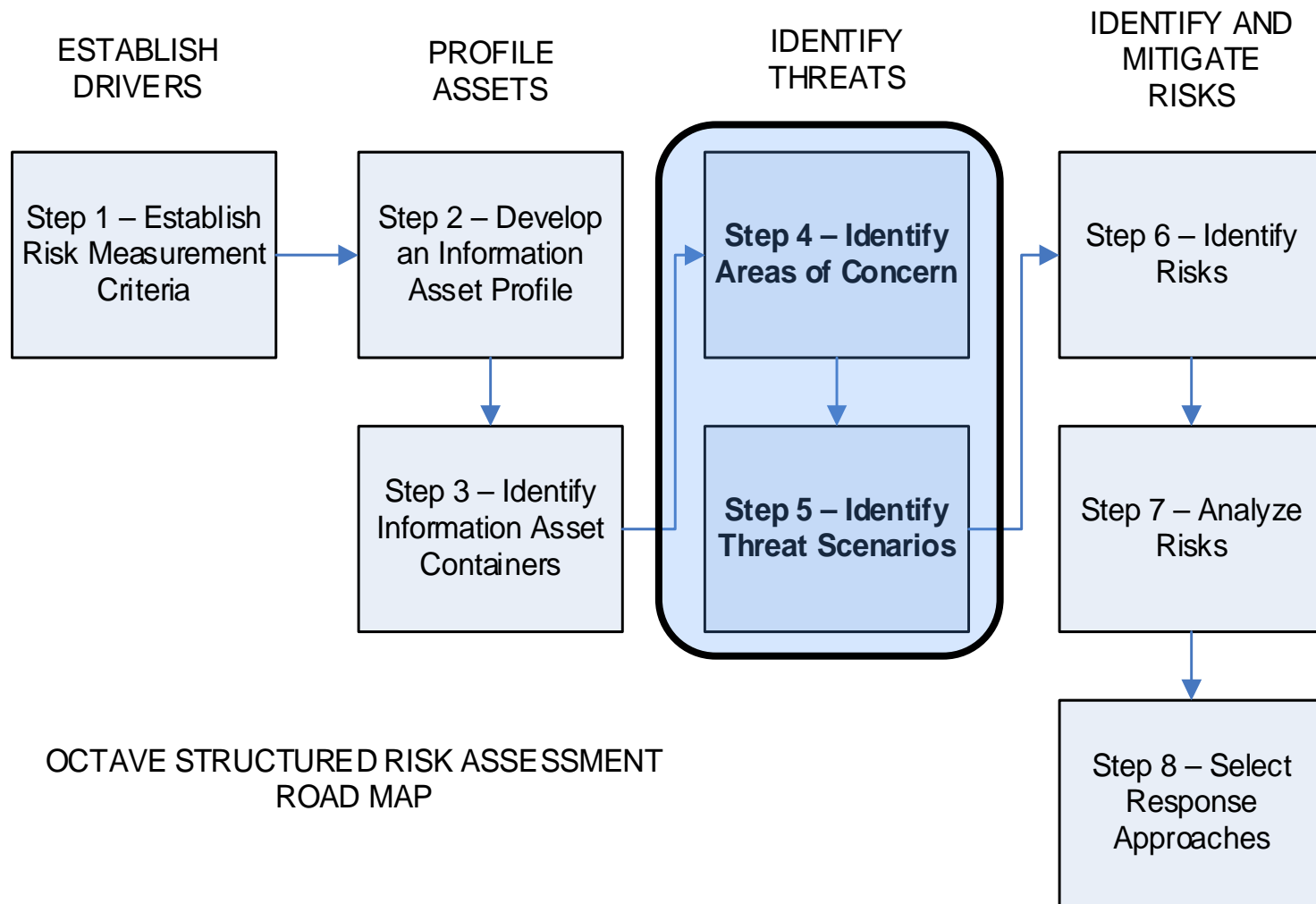
# Leveraging Threat Intelligence in CERT-RMM's Vulnerability Analysis and Resolution (VAR) Process Area



# Leveraging Threat Intelligence in CERT-RMM's Risk Management (RISK) Process Area



# OCTAVE Allegro



OCTAVE STRUCTURED RISK ASSESSMENT  
ROAD MAP

# OCTAVE Allegro

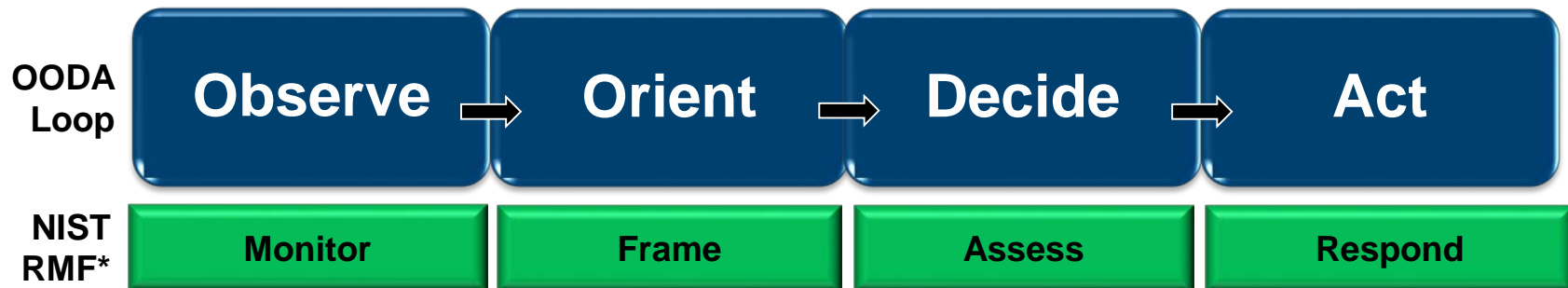
## Information Asset Risk Worksheet

- The information asset
- Area of concern
- Threat actor
- Means
- Motive
- Outcome
- Security requirements
- Probability
- Consequences
- Risk mitigation

# Leveraging Threat Intelligence with NIST Risk Management Framework

A risk management framework, not a controls management framework

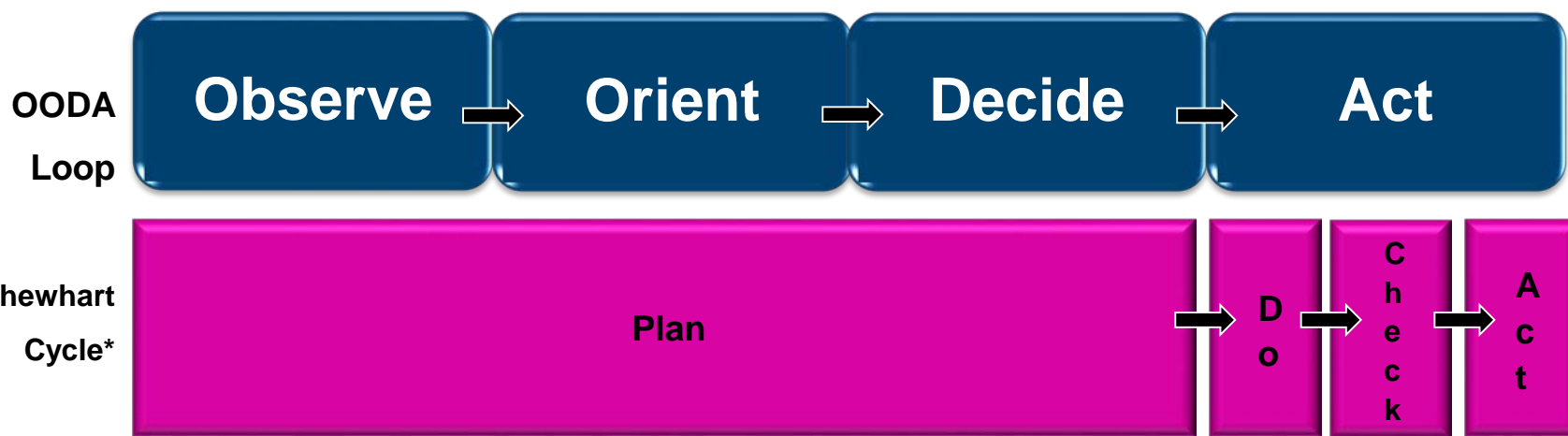
- Tailor controls “with additional controls and/or control enhancements to address unique organizational needs based on...specific threat information”
- Task 5-3 recommends that organizations employ formal or informal risk assessments “to provide needed information on threats, vulnerabilities, and potential impacts as well as the analyses for the risk mitigation recommendations.”



\*Source: NIST SP 800-39. According to NIST SP 800-39, the Risk-Management Process is not a sequential process like the OODA Loop. All components can receive input and send output directly to all other components.

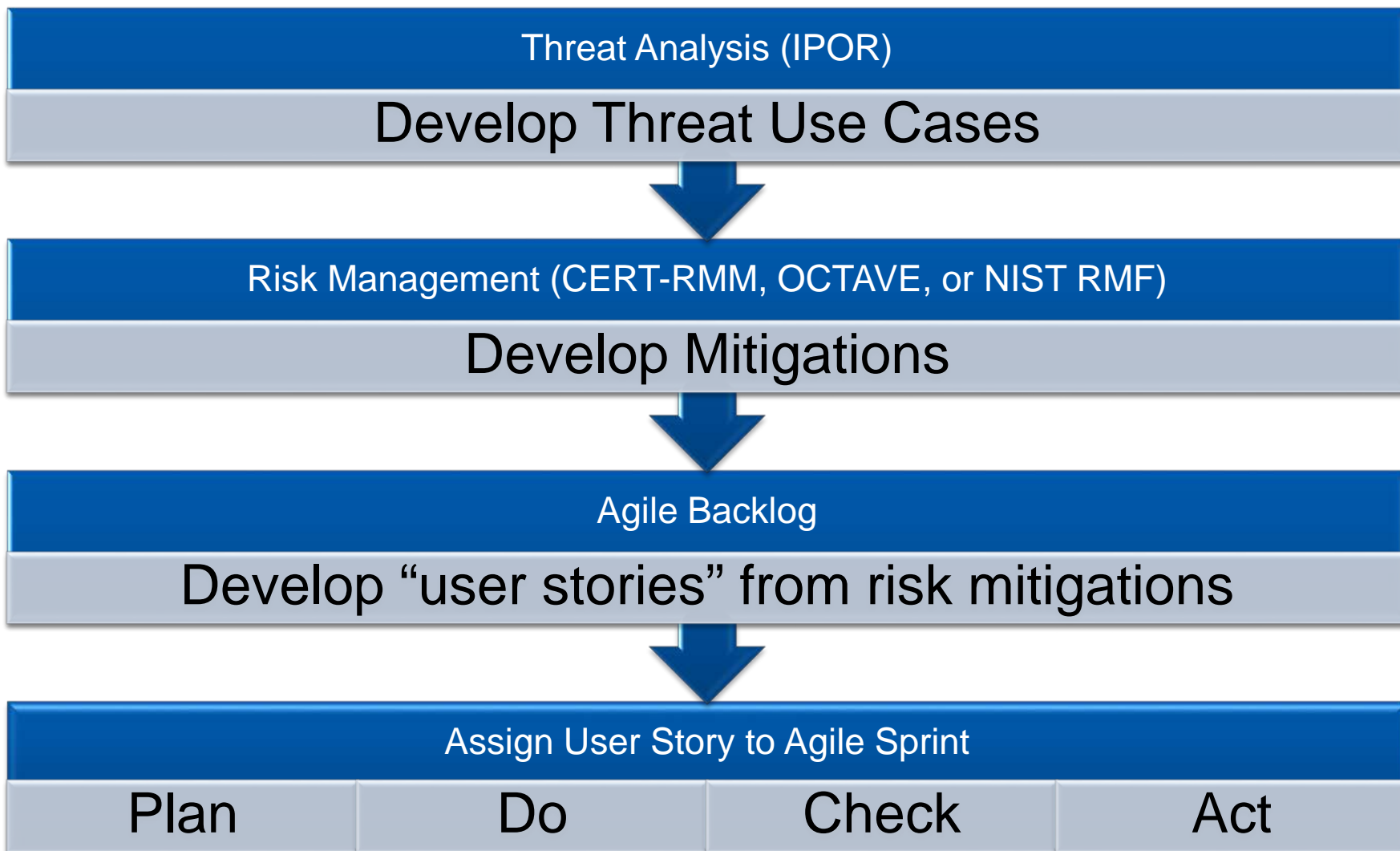
# Leveraging Threat Intelligence with Agile

- Based on the Shewhart Plan-Do-Check-Act cycle
- Emphasizes continuous delivery of functionality
- Functionality is delivered in sprints of approximately one to four weeks
- Requirements are documented in user stories that are then identified from the project backlog for inclusion in the next sprint



\*Source: Walton, M, Deming, W.E. (1988). The Deming Management Method

# Leveraging Threat Intelligence with Agile



# Leveraging Threat Intelligence with Project Management Body of Knowledge (PMBOK)

## Process 4.1

- Use IPOR Results to develop “business case” as part of project charter

## Process 5.1

- Use IPOR results to determine project scope

## Process 5.2

- Use IPOR results to develop requirements
- Can include identifying quality attributes for the system’s architecture

- Developed by the Project Management Institute\*
- Guidelines for managing individual projects\*
- PMBOK consists of six project management process groups and 10 knowledge areas\*
- Responding to mitigating risks based on threat intelligence can be handled like other software projects

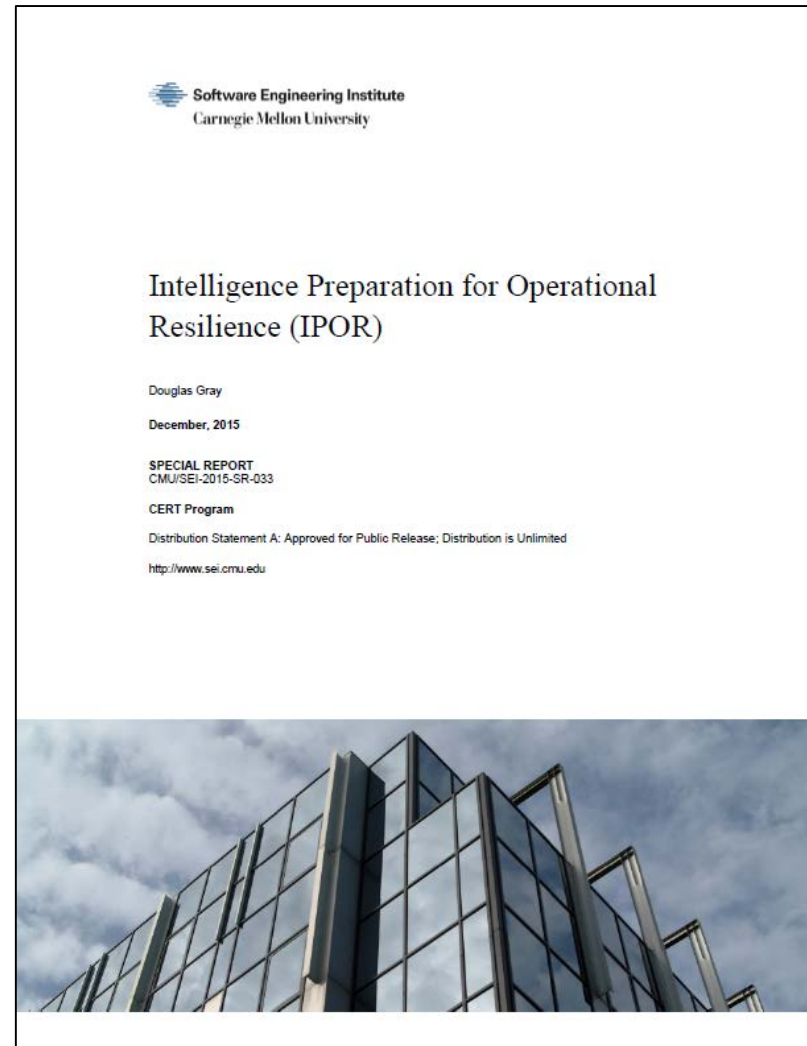
\* Source: A Guide to the Project Management Body of Knowledge (PMBOK®Guide). Project Management Institute (PMI). 2013.

# Conclusion

- Operational resilience practitioners require a method to methodically inject threat-actor intelligence into their resilience, risk, and project-management methodologies,
- IPOR is a way to leverage the IPB process to
  - be accessible to non-DOD, enhance inter-agency and public/private sector information sharing
  - leverage established resilience management model
  - tie directly in with risk-management and project-management frameworks

# For more information

More information on  
IPOR can be found in  
our special report at  
<http://goo.gl/5JzVgL>



# Contact Information

Douglas Gray

Information Security Engineer

Telephone: +1 703.247.1374

Email: [dagray@cert.org](mailto:dagray@cert.org)

Intelligence Preparation for Operational  
Resilience (IPOR)

# Questions



Intelligence Preparation for Operational  
Resilience (IPOR)

# Back Up Slides



Software Engineering Institute

Carnegie Mellon University

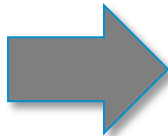
© 2015 Carnegie Mellon University

Distribution Statement A: Approved for Public Release;  
Distribution is Unlimited

# Restating IPB as IPOR

IPB Step	IPB Substep	IPOR Voice	IPOR Substep
Defining the Operational Environment	Identify the limits of the commander's area of operations	Voice of the Organization	Determine the Voice of the Mission
	Identify the limits of the commander's area of interest	Voice of the Environment	All
	Identify significant characteristics of the areas of operations and areas of interest for further analysis	Voice of the Environment	All
	Initiate process necessary to acquire information necessary to complete IPB	Voice of the Environment Voice of the Organization Voice of the Threat	All
Describe environmental effects on operations	Describe how the operational environment influences friendly and threat COAs	Voice of the Environment	All
	So what? - Identify how relevant characteristics of the area of interest will affect friendly and threat operations	Voice of the Environment	All
Evaluate the Threat	Evaluate the threat	Voice of the Threat Actor	Describe the Threat Actor
	Identify threat characteristics	Voice of the Threat Actor	Describe the Threat Actor
Determine Threat Courses of Action	Develop Threat COAs	Voice of the Threat Actor	Determine Threat Use Cases
	Develop event template and matrix	Voice of the Threat Actor	Determine Threat Use Cases

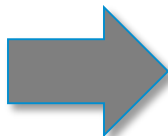
# Tailor Information to Recipient



## Executives:

**C-Suite, elected leaders,  
appointees, generals,  
admirals**

**Target data with eye  
toward organizational  
mission and stakeholders**



## Middle Management:

**Staff, analysts**

**Target data with eye  
toward routines,  
procedures**

[Allison & Zelikow 1999, Kindle locations 3235, 5603]

# Other Management Considerations



- ✓ Build routine, habitual relationship of trust with intelligence provider
- ✓ Formality and rigor will depend on the time and resources available
- ✓ Collect incomplete information and add or revise as more information becomes available
- ✓ Document incorrect information acted upon to illuminate what led to past actions
- ✓ Understand and be able to identify cognitive biases that can distort intelligence

# CERT-RMM Process Areas

Access Management
Asset Definition and Management
Communications
Compliance
Controls Management
Enterprise Focus
Environmental Control
External Dependencies
Financial Resource Management
Human Resource Management
Identity Management
Incident Management & Control
Knowledge & Information Mgmt

Measurement and Analysis
Monitoring
Organizational Process Focus
Organizational Process Definition
Organizational Training & Awareness
People Management
Resiliency Requirements Development
Resiliency Requirements Management
Resilient Technical Solution Engr.
Risk Management
Service Continuity
Technology Management
Vulnerability Analysis & Resolution

# What Is OCTAVE?

A risk-based assessment

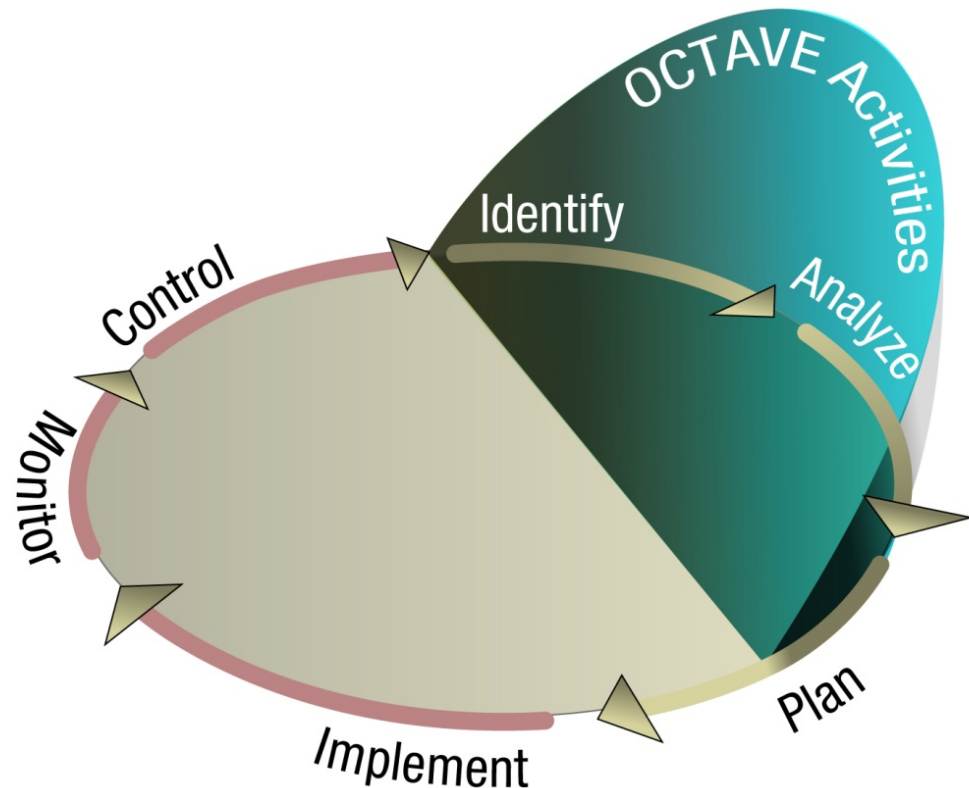
Leverage of people's knowledge of their organization's security-related practices to capture the current state of security practice within the organization

Focused on the asset level

- People
- Information
- Technology
- Facilities
- Supply Chain/Raw Materials

# OCTAVE Approach

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



# 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