Improving Cybersecurity Governance Through Data-Driven Decision-Making and Execution

Doug Gray

© 2014 Carnegie Mellon University

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 OCT 2014	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Improving Cybersecurity Governance Through Data-Driven Decision-Making and Execution	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Douglas Gray	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**26**	

Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security 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 sponsored by 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.

This material has been approved for public release and unlimited 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.

CERT® is a registered mark of Carnegie Mellon University.

DM-0001719

Objectives

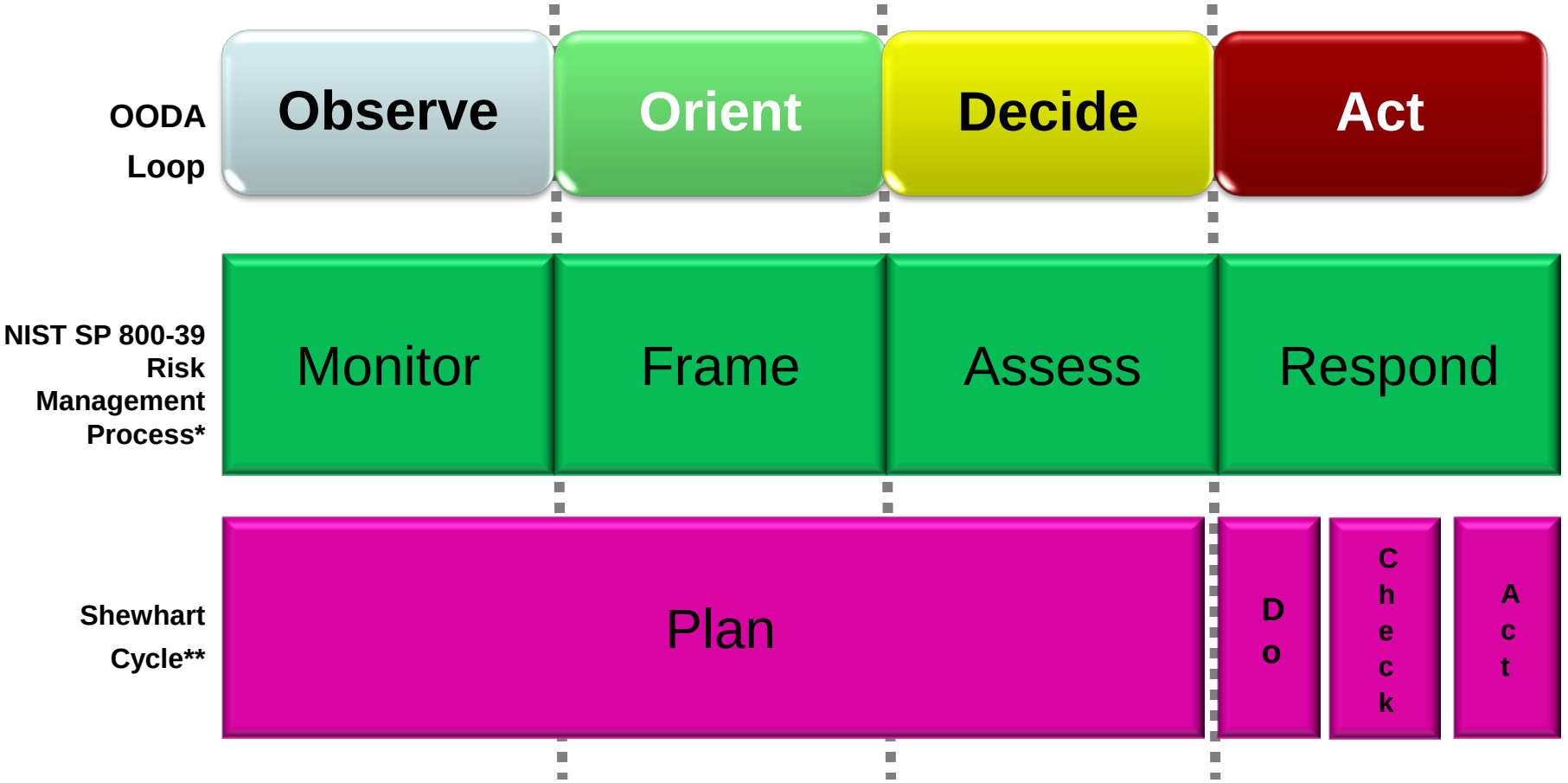
Inform the reader of

- how effective data, metrics, analytics and management can make the Observe-Orient-Decide-Act (OODA) loop faster and more effective
- how a faster and effective OODA loop can make government cybersecurity posture more adaptive and resilient
- how the OODA loop differs between cybersecurity governance and cybersecurity operations
- how to achieve positive cybersecurity governance effects within the OODA framework

The OODA Loop

An Introduction

Comparison of OODA to other Frameworks



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

**Source: Walton (1988)

Why the OODA Loop

- Federal government at inherent cybersecurity disadvantage in comparison to threat actors due to size and structural constraints
- Improved and faster OODA can leverage Federal government's inherent advantages:
  - Economies of scale
  - Opportunities for information sharing
  - Access to law enforcement channels
- Goals:
  - Reduce threat advantage
  - Decrease Federal government's enterprise wide risk surface area
  - Increase cybersecurity governance efficiency
  - Increase threat actors' work factor across the enterprise
- Note: The **Act** phase of the OODA loop does not have to lead to posture-affecting change. It may lead to another, more refined OODA loop.

Cybersecurity Governance

Comparison of Operations and Governance

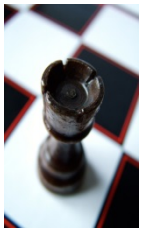
	Operations	Governance
Scope	Individual networks, systems, users, organizations	Multiple networks, systems, user bases, organizations
Timescale	Immediate to 6 months	6 to 36 months*
Level of Abstraction	Transactional	Trends, aggregations
Management Impact	Direct interaction	Context setting

*Although the maximum technology-related decision is limited to approximately three years due to rate of technological change, government organizations must program their expected budget needs five years in advance. In addition, DoD is legislatively mandated to formulate strategy and priorities through the Quadrennial Defense Review process.

Facets of Cybersecurity Governance

Legal, Regulations, Policy, Orders, Investigations & Compliance

Enterprise Risk Management



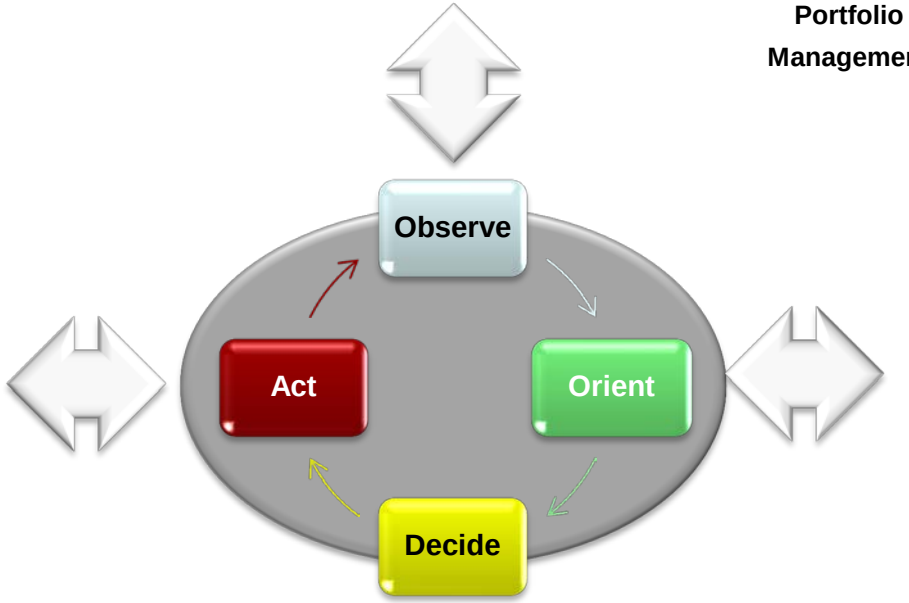
Doctrine & Strategy

Enterprise Portfolio Management

Financial Resource Management

Organizational Training & Awareness

Organizational Structure Management



Enterprise Acquisition & Materiel Management

Human Resources Management & Leader Development

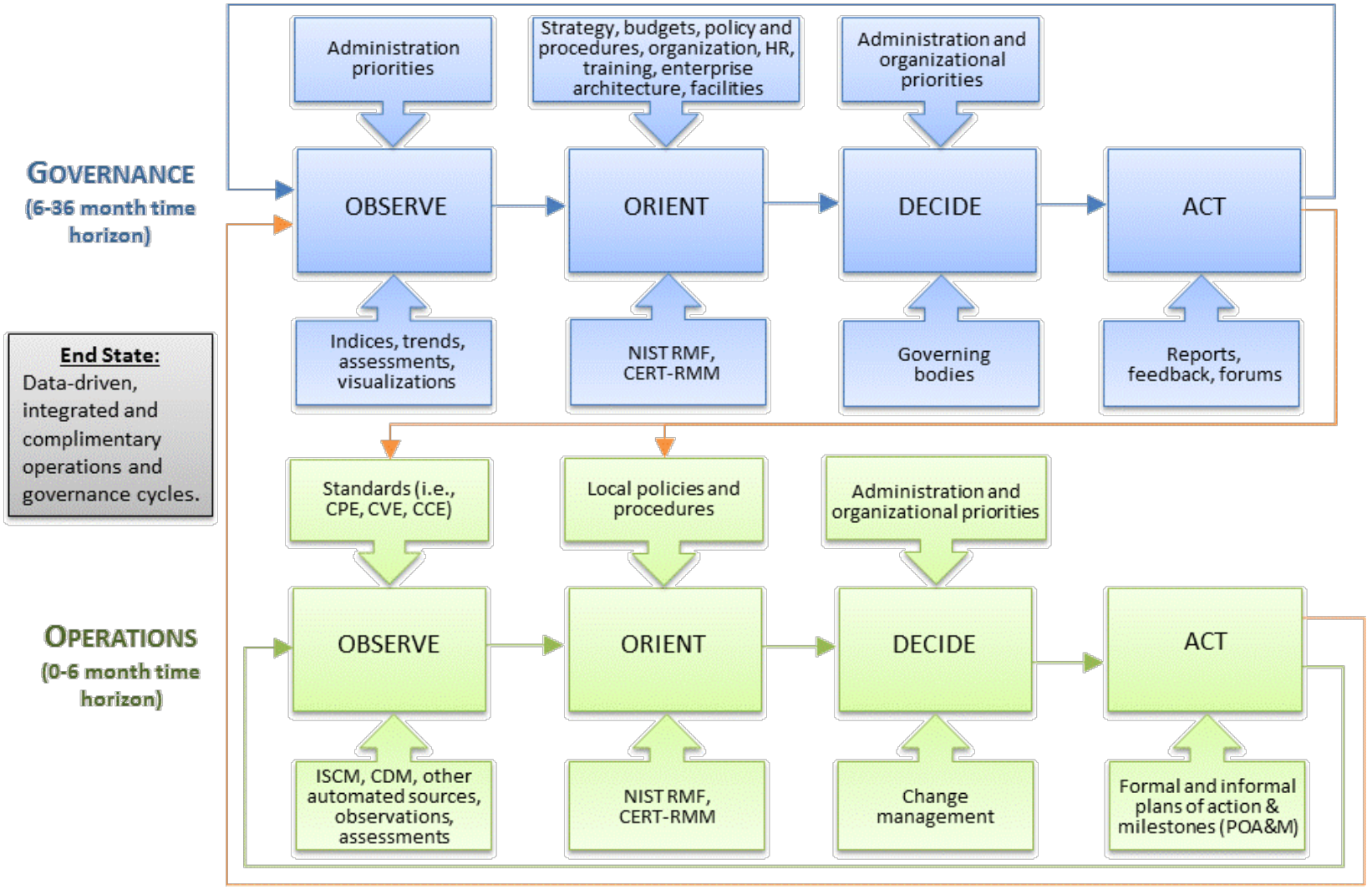
Warfighter Mission Area

Business Mission Area

DoD portion of Intelligence Mission Area

Enterprise Information Environment Mission Area

Using Data to Support Both Governance & Operations Cycles

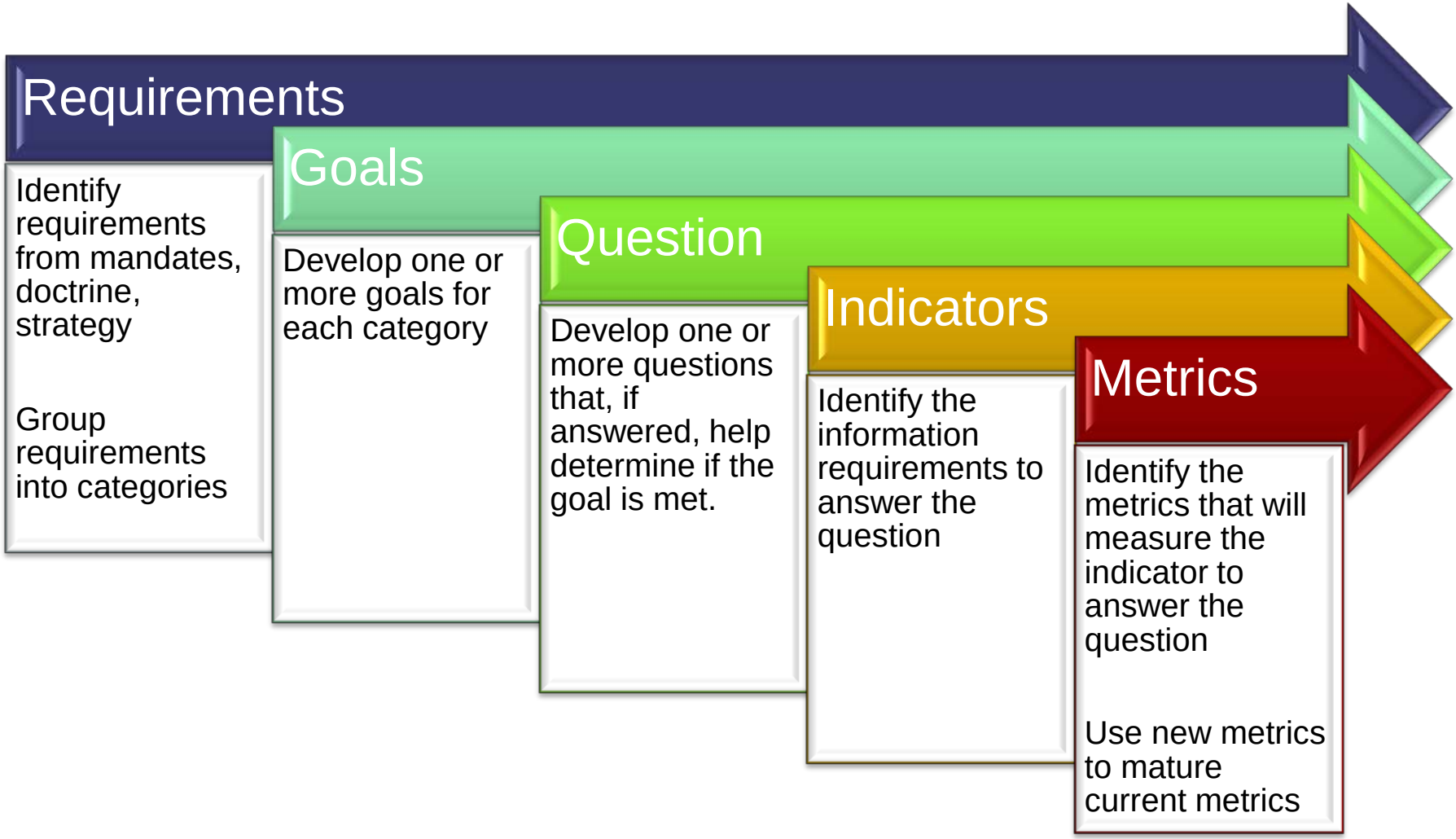


Enabling Data-Driven Decision Making

A faster, more effective OODA Loop

Measure to Support Action

Observe
- Data Collection
- Data Analysis



Collecting Situational Awareness Data and Information

Observe
- Data Collection
- Data Analysis

Automated vulnerability sensor information
- Hardware & Software
- Behavioral Observables (Insider Threat)

Threat Information
- Threat Actor Analysis
- Prevailing Attack Patterns

Management Information
- Budget Information
- Demographic Information
- Legal & Administrative Investigation Statuses
- Mission Impact Analysis

Qualitative Assessment
- Inspections/Assessments
- Professional Sentiments Analysis

Unstructured Data
Machine Learning
Text Analysis
Trend Analysis
Correlation

Orient

Sources of Constraints and Mandates

Orient
- Strategy & Policies
- Norms & Practices

Legislative
- Authority
- Appropriation

FISMA

NDAA

Judicial
- Case law (If applicable)

Google v. United States

United States v. Councilman

Executive
- Executive Order
- OMB Mandate
- FIPS
- Regulations/Military Orders
- Doctrine & Strategy
- Recommendations/Guides

Executive Order 13587

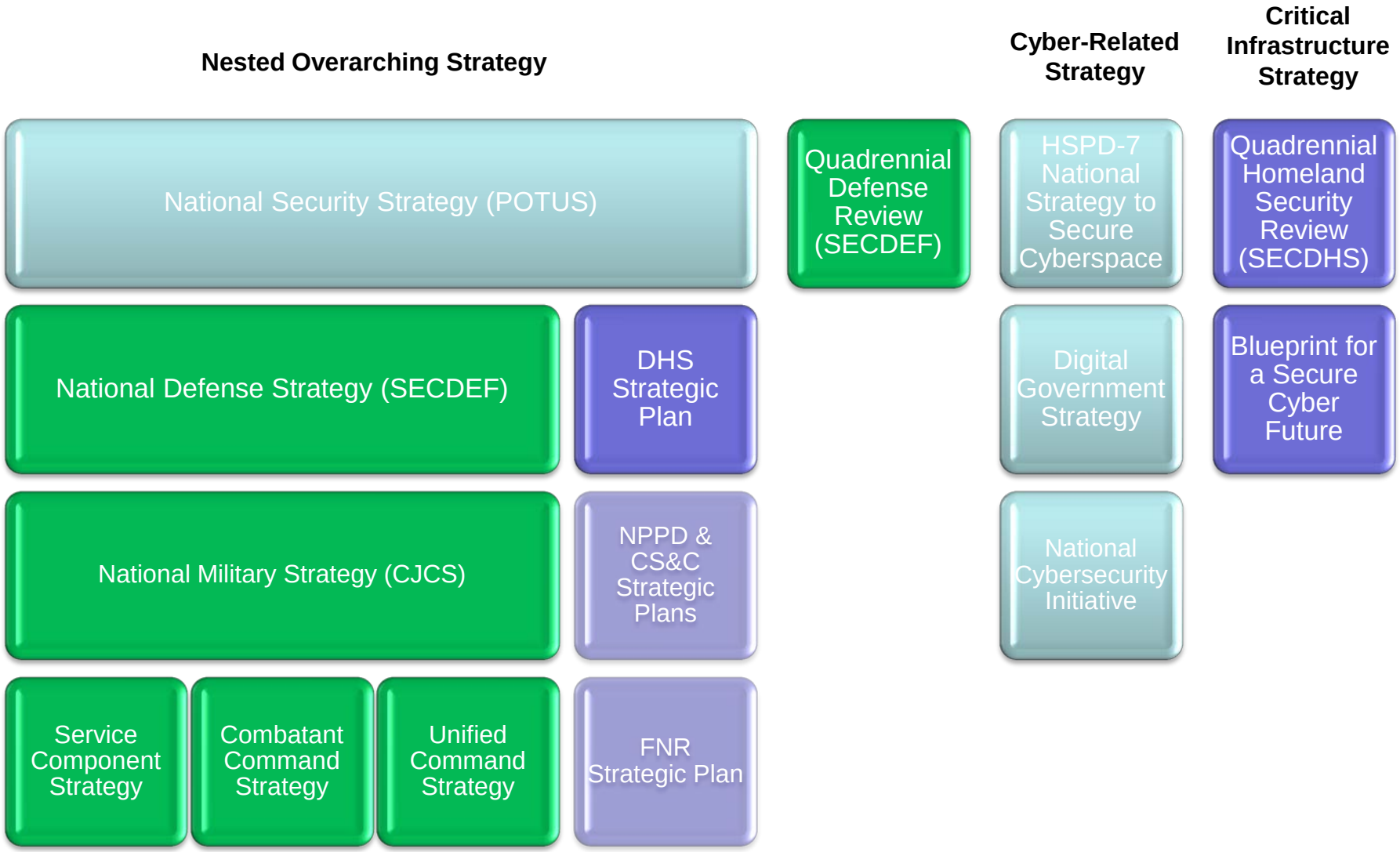
DODD 8570.X/ 8140

DISA CRMS

STIGs/ NIST SPs

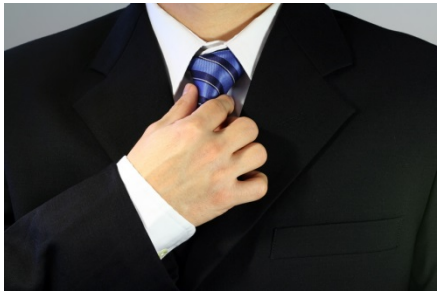
Government Strategy Landscape

Orient
- Strategy & Policies
- Norms & Practices



Use Behavioral Models to Target Stakeholder Information Needs

Orient
- Strategy & Policies
- Norms & Practices



Executives:
- Elected leaders, appointees, GOs, FOs, SESs
- Target data with eye toward organizational mission and stakeholders

Middle Management:
- Staff officers, analysts
- Target data with eye toward routines, procedures

Source: Allison, G. T., & Zelikow, P. (1999). *Essence of Decision: Explaining the Cuban Missile Crisis* (2nd ed.) (Kindle Edition). New York: Longman.

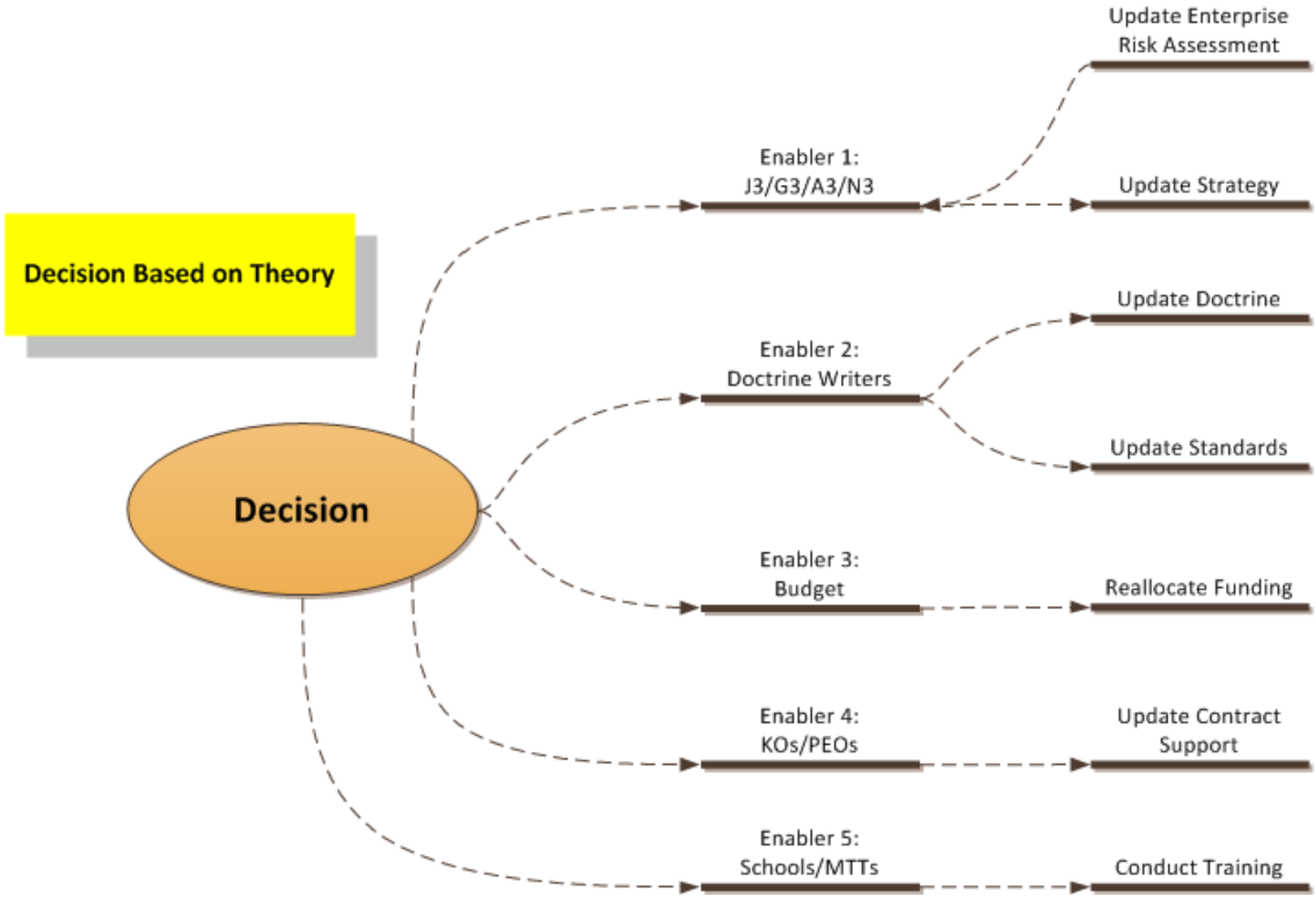
Key Planning & Decision-Making Factors

Decide
- **CoA Development**
- **Planning**

- Theory or hypothesis?
  - Hypothesis – analyze through subsequent OODA loop
  - Theory – develop action plan to effect change
- Identify and prioritize governance-level risks; identify metric-supported thresholds of acceptability and unacceptability
- Support solutions. Go beyond "name and shame". Use metrics to identify key trends and corrective governance-level actions
- Tie metrics to a resulting set of possible risk management outcomes
- Identify enablers such as SMEs, funding, contract vehicles
- Identify organizations that exceed expectations in certain areas and their lessons learned
- Identify what expected changes in metric values should be and how to avoid bias/gaming
- Prioritize and identify metric thresholds where costs will exceed benefits.

Leveraging Enablers to Achieve Desired Effects

Act
- Execution
- Follow-Up



Success at the Point of Execution

Act
- Execution
- Follow-Up

- Leverage enablers at the proper organizational level; avoid the “3,000-mile screwdriver”
- Governance sets the direction through governance facets. Operations executes through disciplined project management
- Avoid numerous, rapid changes that cause enterprise turbulence
- Tie actions to expected outcomes and expected timeframes; socialize and communicate expectations
- Set decision points to check progress against expectations
- Build knowledge base to make for faster and more effective OODA loop

How to Implement

Observe

- Inventory on-hand data
- Inventory metrics
- Develop data fusion capabilities

Orient

- Refine metrics based on constraints, mandates, threat patterns
- Define stakeholders based on behavioral models
- Develop quantitative and qualitative analysis engines
- Develop visualization capabilities

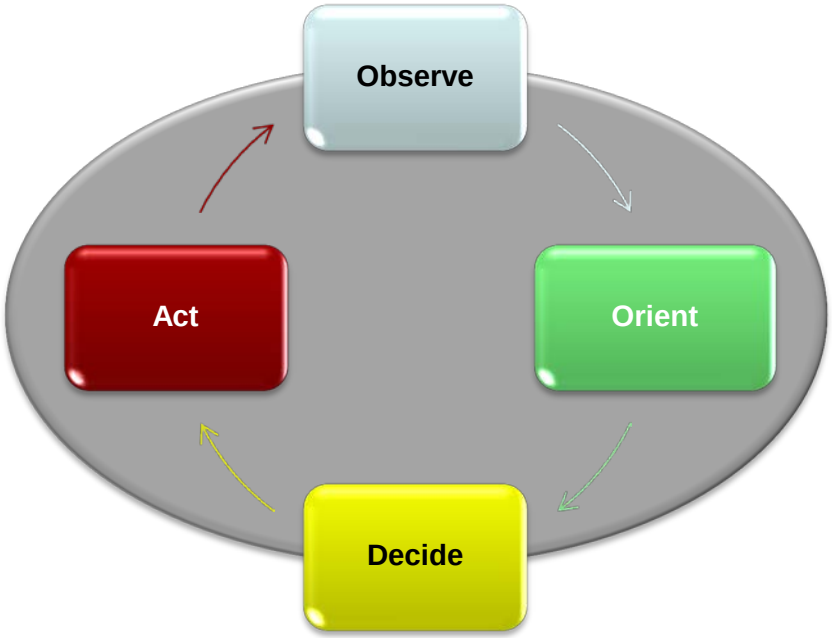
Decide

- Inventory enablers and their capabilities
- Identify desired outcomes for metrics (i.e. thresholds)
- Develop decision support TTPs
- Develop decision-support systems

Act

- Develop knowledge base
- Simulate and practice new decision-making TTPs
- Develop and refine process control mechanisms
- Develop, refine and leverage communications channels

Outcomes of Data Driven Governance



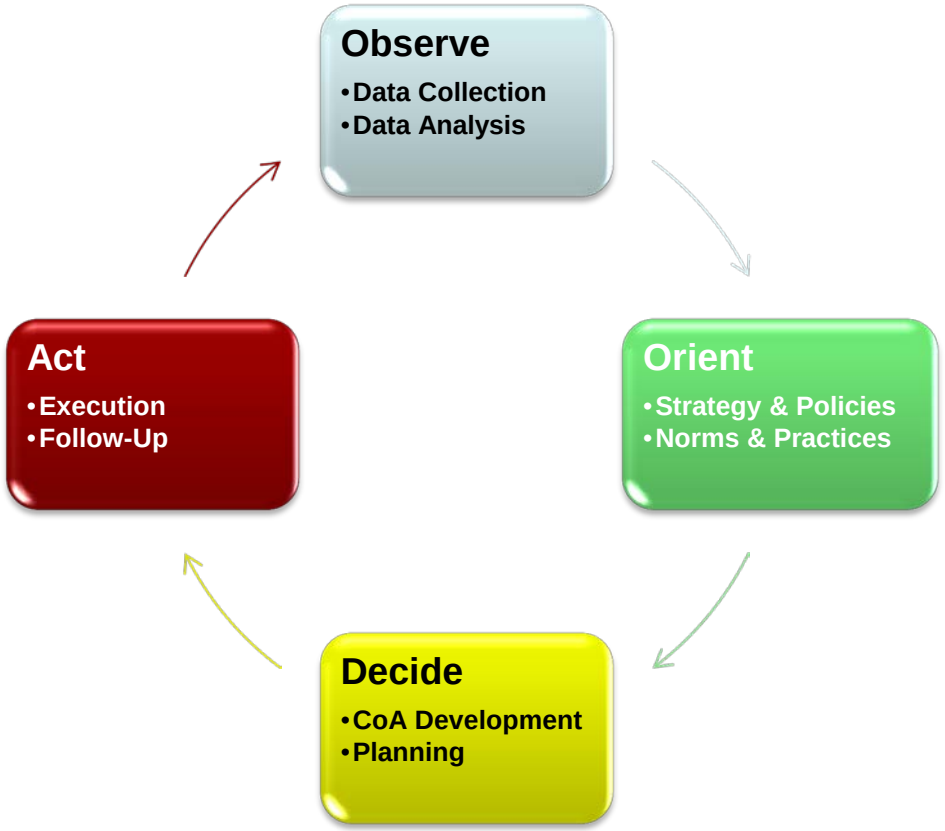
- Faster, more accurate decision making
- Better use of resources
- Better enterprise cohesion and synchronization
- Data-driven outcomes
- Improved information sharing
- Adaptable to change

Questions

Back-Up Slides

The OODA Loop

- Mental model for conceptualizing how individuals, organizations make decisions
- Origins in the DoD; used in legal and business communities
- Describes the ability to acquire, process and act up on information with respect that that of one's adversary



The OODA Loop

- **Observe**: Gathering sensory inputs from the environment of the observer
- **Orient**:
  - Make sense of the observational data to create a mental picture of the situational reality
  - Used to make sense of the input data in light of what is "known"
  - Provides the basis for decisions
- **Decide**: Deciding on a course of action based on Orientation
- **Act**: Bringing decision to fruition at point of execution.

Source: Angerman (2004)

References

- Angerman, W.S., (2004). Coming Full Circle with Boyd's OODA Loop Ideas: An Analysis of Innovation Diffusion and Evolution, Mar 2004
- Caralli, R.A., Allen, J.H., White, D.W. (2010). CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience
- Walton, M, Deming, W.E. (1988). The Deming Management Method
- NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Life Cycle Approach (2010). Department of Commerce (NIST)
- NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View (2011). Department of Commerce (NIST)
- Blueprint for a Secure Cyber Future (2011). Department of Homeland Security
- Quadrennial Homeland Security Review Report (2010). Department of Homeland Security
- Allison, G. T., & Zelikow, P. (1999). Essence of Decision: Explaining the Cuban Missile Crisis (2nd ed.) (Kindle Edition). New York: Longman.