SEI Measurement Project

Carol Woody, Ph.D.

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Software Engineering Institute | Carnegie Mellon

SEI Approach

Provide solutions that enable organizations to

- Effectively measure their current state with respect to software assurance
- Evaluate their options and tradeoffs
- Select solutions based on their highest-priority risks
- Implement the selected solutions

Software must effectively support the operational mission

Definitions

Measurement

A quantitatively expressed reduction of uncertainty based on one or more observations[1]

1. Hubbard, Douglas. *Applied Information Economics Seminar: Executive Overview*. Hubbard Decision Research, 2010. http://www.hubbardresearch.com/

Software Assurance (Software Assurance Curriculum Project)

Application of technologies and processes to achieve a required level of confidence that software systems and services function in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures.

Software Measures: *Examples of Current State of Practice*[1]

>90% applications and data assets evaluated for risk classification in past 12 months

>60% development staff trained within past 1 year

>80% staff certified within past 1 year

>50% of projects with updated attack surface analysis in past 12 months

>50% of projects with updated security requirements design-level analysis in past 12 months

>50% of project teams performing code review on high-risk code in past 6 months

1. *Software Assurance Maturity Model, Version 1.0*. Open Web Application Security Project (OWASP). http://www.opensamm.org/

SEI Approach: Two-Tiered Measurement and Analysis

Systemic Measures (effectiveness)

Tactical Measures (implementation)

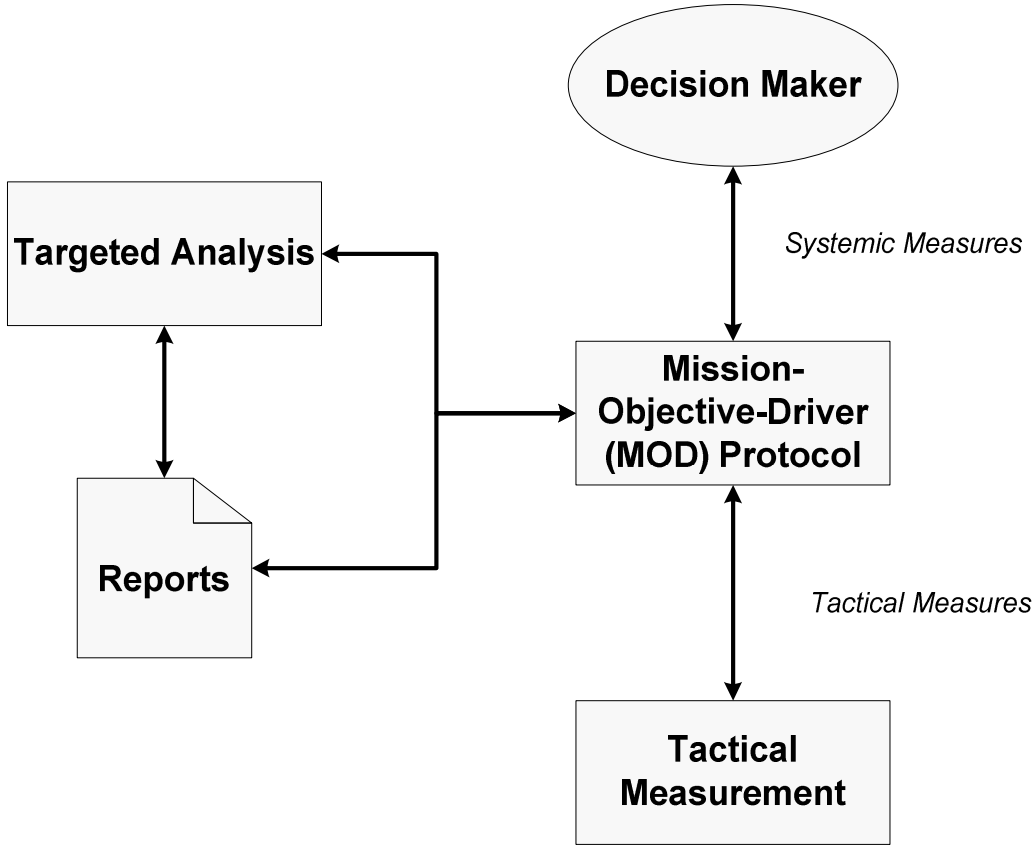
A measure that provides a decision maker with insight into the overall performance of a socio-technical system (based on systemic analysis).

Example: 10% probability that the code will be sufficiently secure.

A measure that provides a decision maker with insights into a specific task that must be performed or some characteristic of a work product.

Example: >50% of project teams performing code review on high-risk code

Integrated Measurement and Analysis Framework (IMAF)



The MOD Protocol implements systemic analysis.

IMAF provides decision makers with insight into the mission.

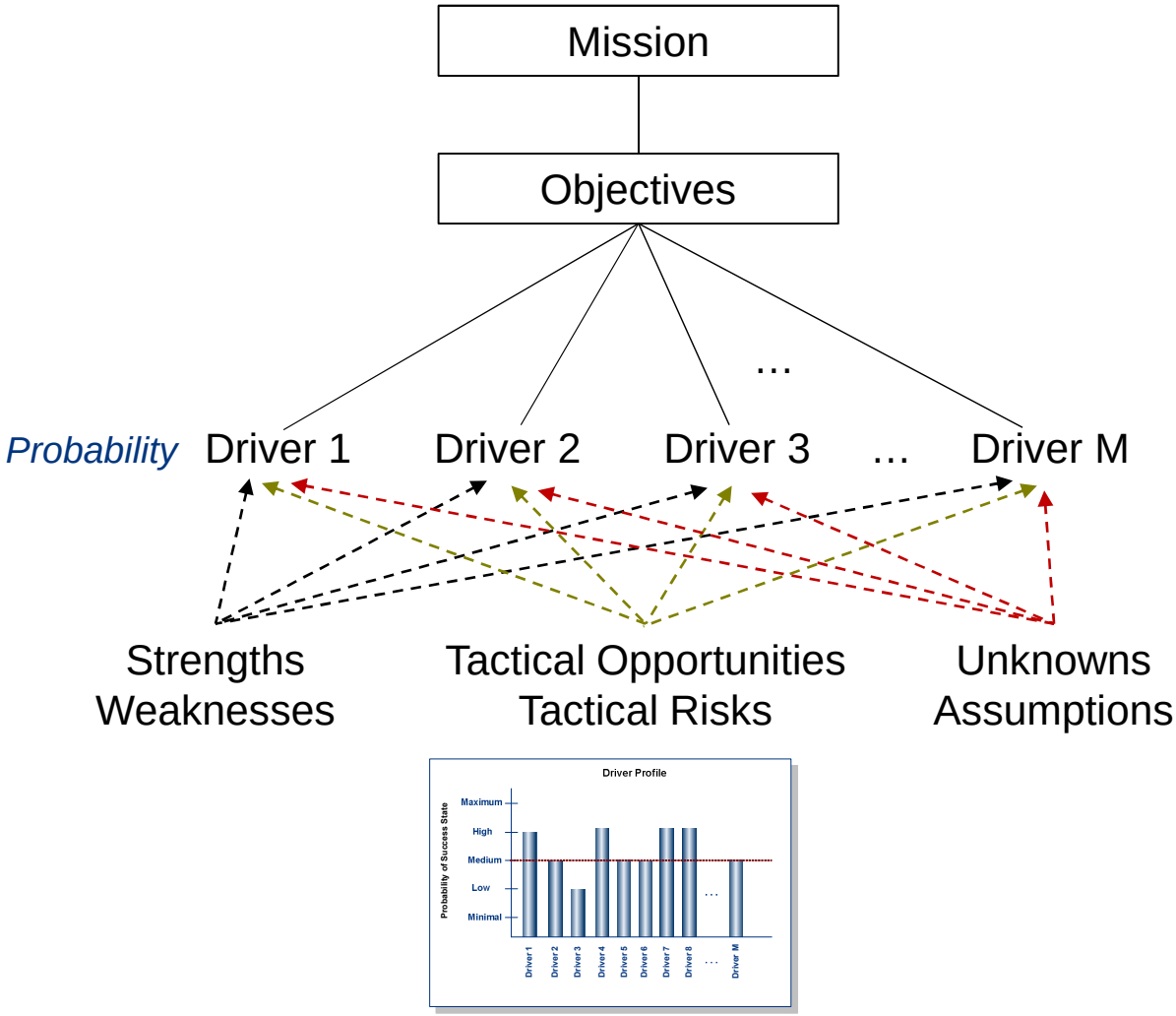
Mission-Objective-Driver (MOD) Protocol: *Systemic Analysis of Mission and Objectives*

Driver Identification

1. ***Identify the mission.***
2. ***Identify objectives.***
3. ***Identify drivers (i.e., critical factors that have a strong influence on outcome or result).***

Driver Analysis

4. ***Evaluate drivers.***
5. ***Document evidence.***
6. ***Establish driver profile.***



Standard Driver Framework for Secure Software Development (Draft)

Objectives

1. Program Security Objectives

Preparation

2. Security Plan
3. Contracts
4. Security Process

Execution

5. Security Task Execution
6. Security Coordination
7. External Interfaces

Environment

8. Organizational and External Conditions

Resilience

9. Event Management

Result

10. Security Requirements
11. Security Architecture and Design
12. Code Security
13. Operational System Security
14. Adoption Barriers
15. Operational Security Compliance
16. Operational Security Preparedness
17. Security Risk Tolerance

Evaluating Drivers

Directions: Select the appropriate response to the driver question.

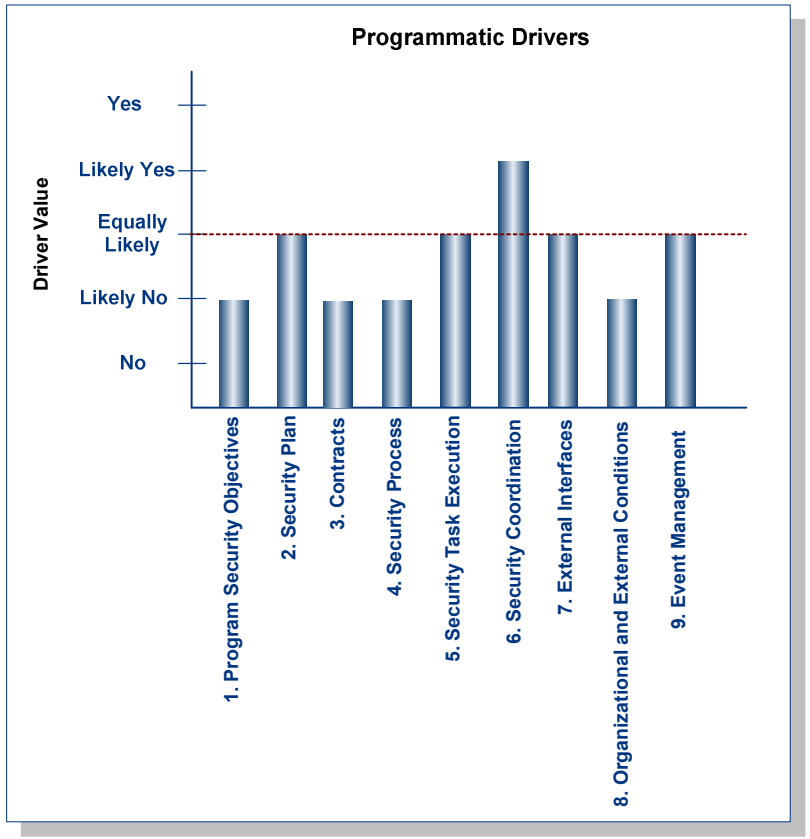
Driver Question	Response
4. Does the process being used to develop and deploy the system sufficiently incorporate security? *Consider:* ▪ Security-related tasks and activities in the program workflow ▪ Conformance to security process models ▪ Measurements and controls for security-related tasks and activities ▪ Process efficiency and effectiveness ▪ Software security development life cycle ▪ Security-related training ▪ Compliance with security policies, laws, and regulations	❑ Yes ❑ Likely Yes ❑ Equally Likely X Likely No ❑ No ❑ Don't Know ❑ Not Evaluated

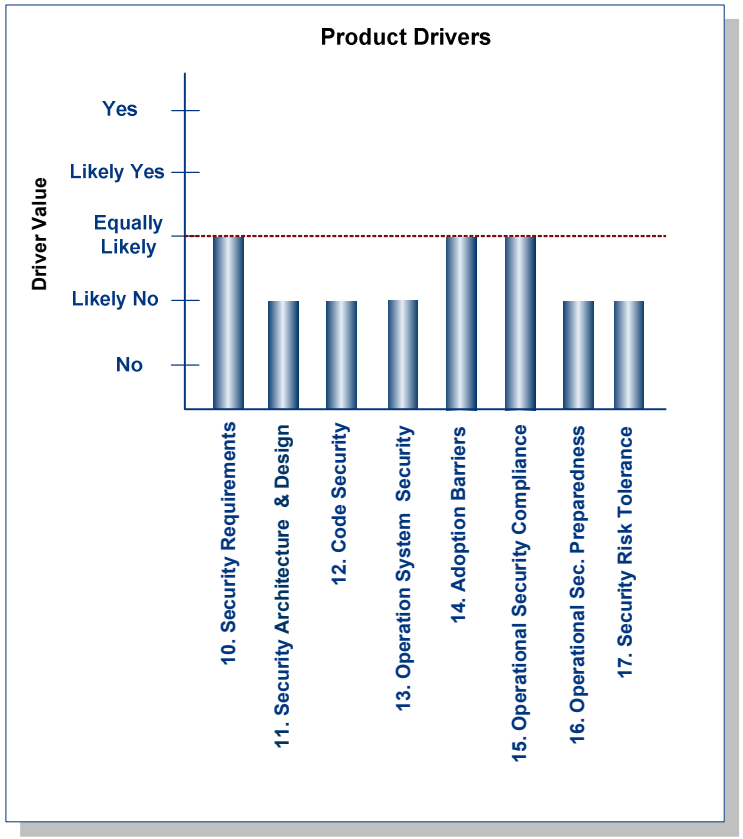
Driver questions are phrased from the success perspective.

Probability is incorporated into the range of answers for each driver.

The rationale for selecting an answer is recorded.

Driver Profile

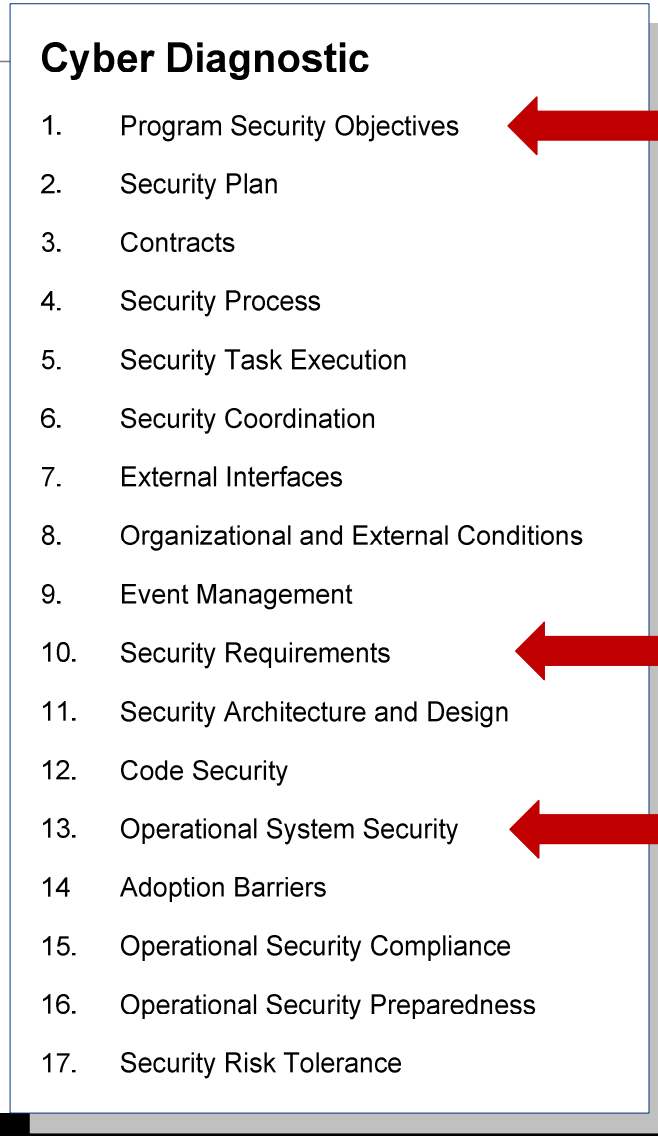




A driver profile provides a snapshot of current conditions.

The driver profile provides a dashboard for program decision makers.

Cyber Diagnostic



Security Investment Decision Dashboard (SIDD) helps shape a program's security objectives by analyzing tradeoffs for security investments.

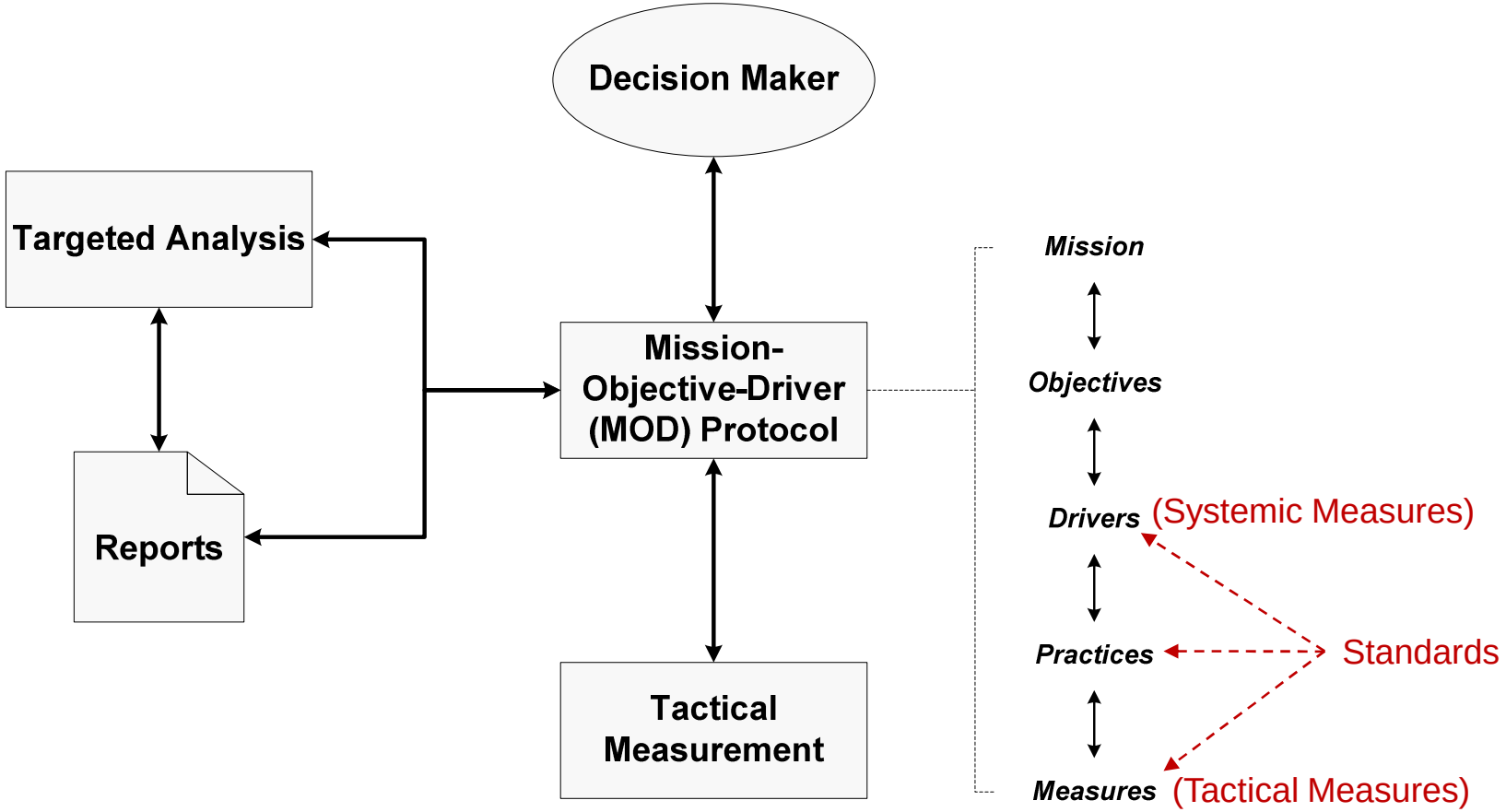
The Cyber Diagnostic provides a broad view of the security mission.

Other methods can be used to provide deep dives.

Security Quality Requirements Engineering (SQUARE) is a method for identifying and prioritizing security requirements.

Survivability Analysis Framework (SAF) is a method for identifying and addressing gaps, inconsistencies, and potential failures between design and operation.

Mapping: *Practices, Standards, and Measures*



The mapping aligns practices, standards, and measures with the mission.

Example: *NIST 800-53 -1*

Family and Class	Control	Related Controls
SI. System and Information Integrity	SI-2 Flaw Remediation The organization: a) Identifies, reports, and corrects information system flaws; b) Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c) Incorporates flaw remediation into the organizational configuration management process.	CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11

Example: *NIST 800-53 -2*

Guidance	Related Drivers	Practices	Measures
2. The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Organizations are encouraged to use resources such as the Common Weakness Enumeration	16. Operational Security Preparedness 7. External Interfaces	Security-relevant software updates are installed for all software components with software flaws and vulnerabilities where corrective action is required. Security-relevant software updates are installed in a timely manner. "Updates" as used here may also include other mitigating actions that do not involve a change to the software.	• % of software components requiring security-relevant software updates • % of software components requiring security-relevant software updates where such updates have been installed

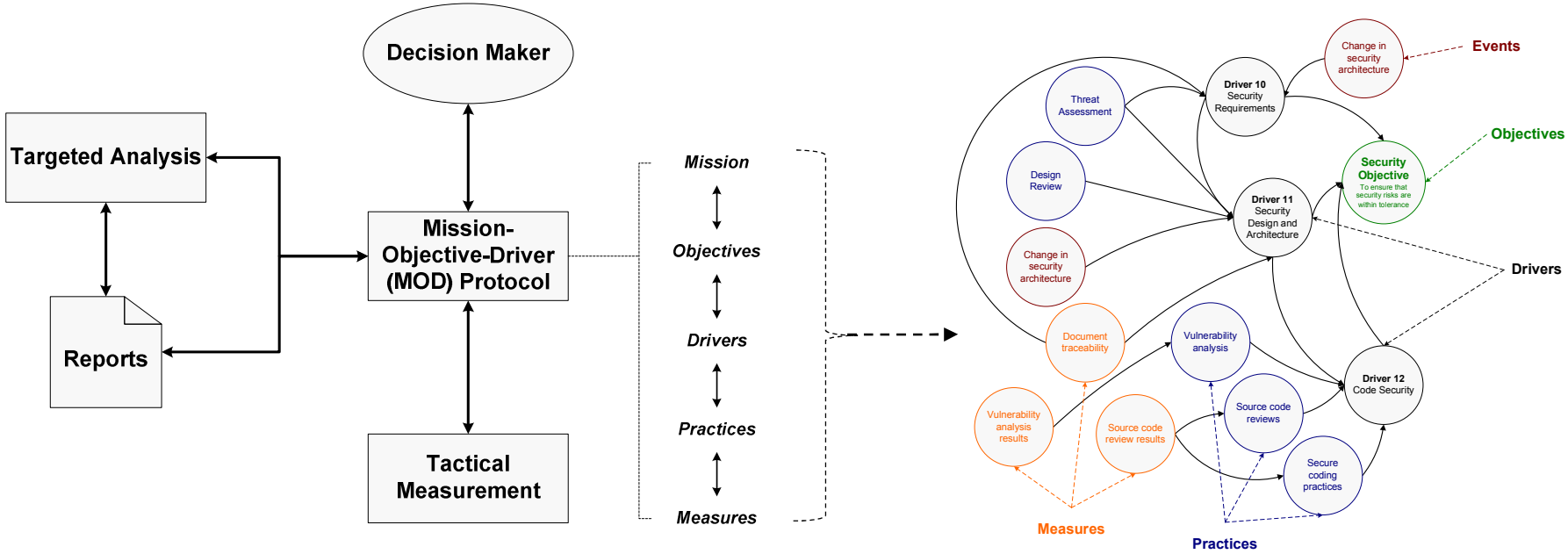
Example: *ISO 27002 -1*

Security Clause	Security Topic	Control Objective	Control
12. Information systems acquisition, development and maintenance	12.1. Security requirements of information systems	To ensure that security is an integral part of information systems	12.1.1 Security requirements analysis and specification Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.

Example: *ISO 27002 -2*

Guidance	Related Driver	Practice	Measures
2. Security requirements justified, agreed, and documented as part of the business case for an information system (Objective)	10. Security Requirements	Security requirements are documented as part of the business case	• % of system components for which security requirements are/are not documented as part of the business case for the information system • % of business cases for information systems that include/do not include security requirements for the system components that reside on the system

Modeling and Simulation: *Bayesian Belief Networks*



Bayesian Belief Network

A Bayesian Belief Network can be used to establish quantitative probabilities.

Effective Capability for Now and Beyond

Blending of qualitative and quantitative measures (proof of concept)

- Provide the right questions to ask vendors and developers about assurance
- Identify effective evidence and artifacts that support assurance

Building line of site from organizational mission to security standards and practices for measurement

- Extend beyond responses to individual problems
- Integrate decision-making framework into normal operations to measure and monitor over time

References

Measurement Report

"Integrated Measurement and Analysis Framework for Software Security"

http://www.sei.cmu.edu/reports/10tn025.pdf

Mission Assurance Reports

"Preview of the Mission Assurance Analysis Protocol (MAAP): Assessing Risk and Opportunity in Complex Environments"

http://www.sei.cmu.edu/reports/08tn011.pdf

"A Framework for Categorizing Key Drivers of Risk"

http://www.sei.cmu.edu/reports/09tr007.pdf

Contact Information

Carol Woody

(412) 268-9137

cwoody@cert.org

Web Resources (CERT/SEI)

http://www.cert.org/

http://www.sei.cmu.edu/