Solutions. Experts. Insights.

SEI TECHNOLOGIES FORUM

Software Engineering Institute | Carnegie Mellon

Measuring Operational Resilience

Julia Allen
CERT

Allen is a principal researcher within the CERT Program at the SEI. Allen's areas of interest include operational resilience, software security and assurance, and measurement and analysis. Prior to this technical assignment, Allen served as acting director of the SEI for an interim period of six months as well as deputy director/chief operating officer for three years.

.

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
24 OCT 2011

2. REPORT TYPE

3. DATES COVERED
00-00-2011 to 00-00-2011

4. TITLE AND SUBTITLE
Measuring Operational Resilience

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Carnegie Mellon University ,Software Engineering Institute,Pittsburgh,PA,15213

8. PERFORMING ORGANIZATION REPORT NUMBER

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

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	17. LIMITATION OF ABSTRACT **Same as Report (SAR)**	18. NUMBER OF PAGES **30**	19a. NAME OF RESPONSIBLE PERSON

Topics

CERT Resilience Management Model Overview

What Is the Question? What Should I Measure?

Measurement Defined

Key Measures

Getting Started

CERT-RMM Overview

What is CERT®-RMM?

The CERT® Resilience Management Model is a maturity 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

- **Process improvement for operational resilience**
- **Converges key operational risk management activities: security, BC/DR, and IT operations**
- **Defines maturity through capability levels *(like CMMI)***
- **Improves confidence in how an organization responds in times of operational stress and disruption**

CERT-RMM: 26 Process Areas in 4 Categories

Engineering

ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management

COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training & Awareness
RISK	Risk Management

Operations Management

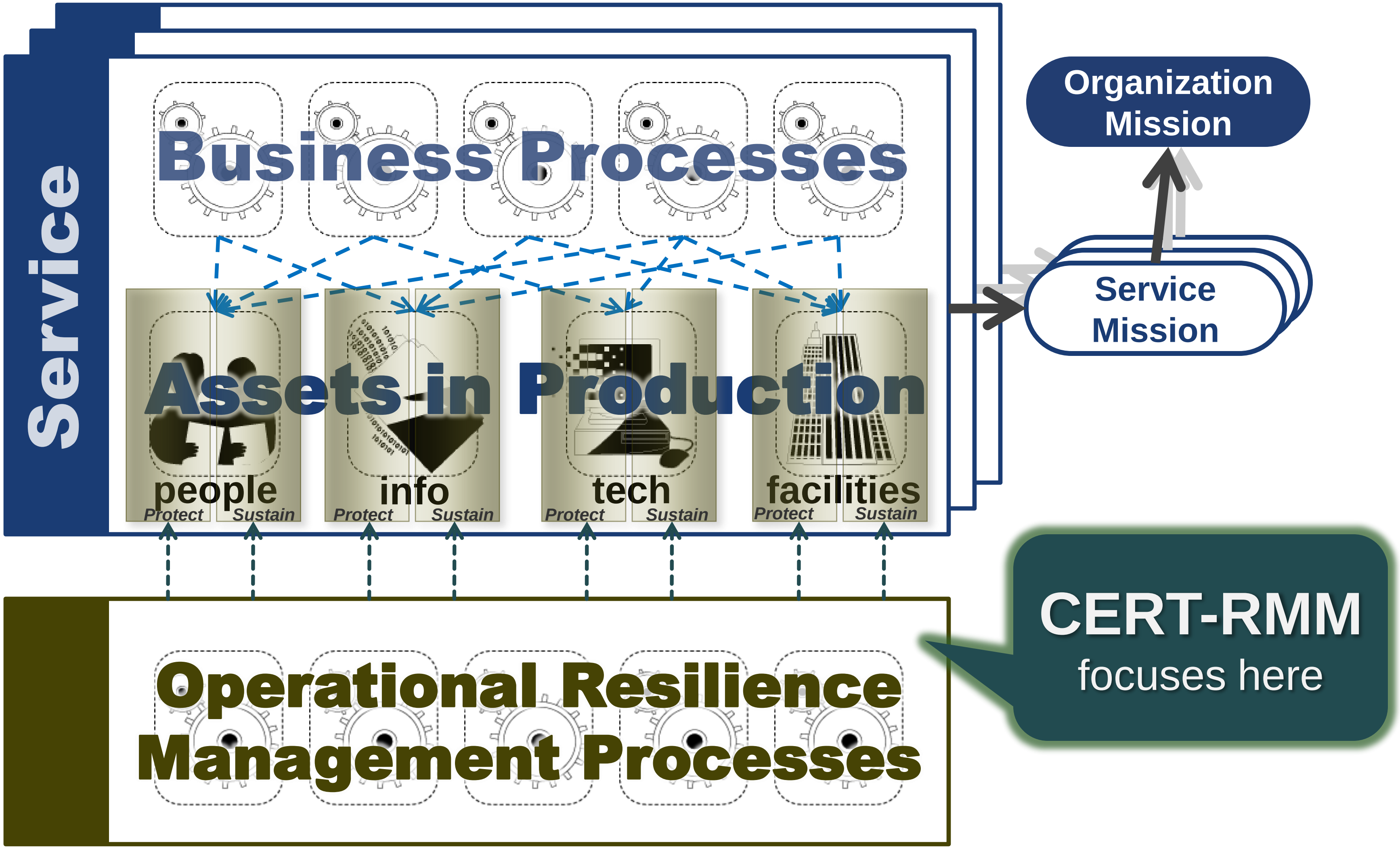
AM	Access Management
EC	Environmental Control
EXD	External Dependencies
ID	Identity Management
IMC	Incident Management & Control
KIM	Knowledge & Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis & Resolution

Process Management

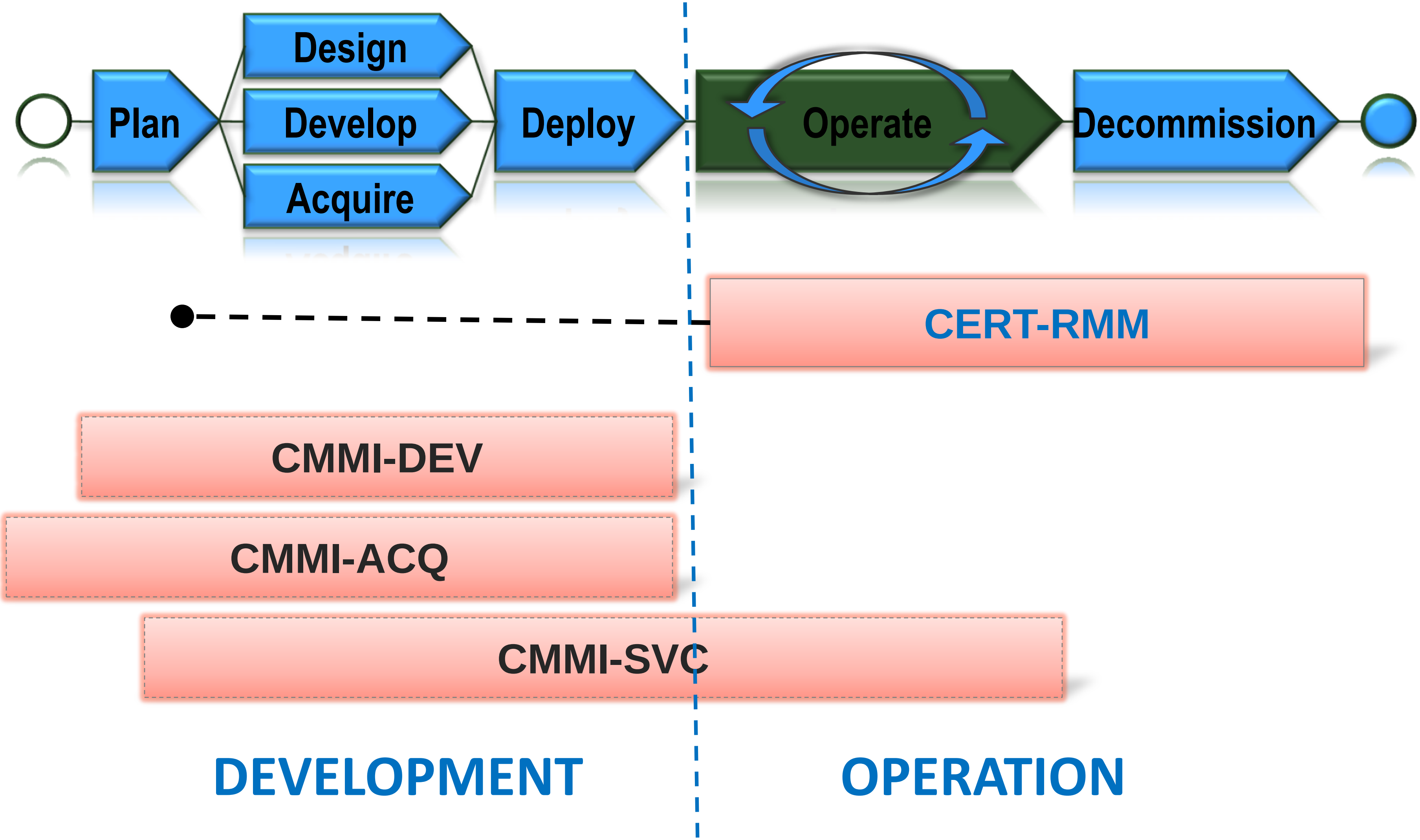
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus

Full text of each process area is available for download at www.cert.org/resilience

Organizational Context



For Comparison: CERT-RMM & CMMI



What Is the Question?
What Should I Measure?

How Resilient Am I? - 1

When asked:

- How resilient am I?
- Am I resilient enough?
- How resilient do I need to be?

What does this mean?

How Resilient Am I? - 2

- Do I need to worry about operational resilience?
- If services are disrupted, will it make the news? Will I end up in court? in jail? Will I be able to stay in business?
- Do I meet compliance requirements?
- How resilient am I compared to my competition?
- Do I need to spend more $$ on resilience? If so, on what?
- What am I getting for the $$ I've already spent?

How Resilient Am I? - 3

What should I be measuring to determine if I am meeting my performance objectives for resilience?

What is the business value of being more resilient?

So What? Why Should I Care? (*)

- What decisions would this measure inform?
- What actions would I take based on it?
- What behaviors would it affect?
- What would improvement look like?
- What would its value be in comparison to other measures?

(*) informed by Douglas Hubbard, *How to Measure Anything*, John Wiley & Sons, 2010

What Should I Measure?

Determine **business objectives** and key questions

Define the **information** that is needed to answer the question

Qualify and quantify the information in the form of measures

Analyze the measures and report out

Quantify the **value** of each measure (cost/benefit)

Refine and retire measures as you go

Who, What, Where, When, Why, How

Who is the measure for? Who are the stakeholders? Who collects the measurement data?

What is being measured? As part of what process?

Where is the data/information stored?

When/how frequently are the measures collected?

Why is the measure important (vs. others)? The most meaningful information is conveyed by reporting trends over time vs. point in time measures.

How is the data collected? How is the measure presented? How is the measure used?

Measurement Defined

Measurement Types

Implementation

- Is this process/activity/practice being performed?

Effectiveness

- How good is the work product or outcome of the process/activity/practice? Does it achieve the intended result?

Process performance

- Is the process performing as expected? Is it efficient? Can it be planned? Is it predictive? Is it in control?

Measurement Template

- Measure Name/ID
- Goal
- Question(s)
- Related Processes/ Procedures
- Visual Display
- Data Input(s) (Data elements, Data type)
- Data Collection (How, When, How often, By whom)
- Data Reporting (By, To whom, When, How often)
- Data Storage (Where, How, Access control)
- Stakeholders (Information owner(s), collector(s), customer(s))
- Algorithm or Formula
- Interpretation or Expected Value(s)

A Few Strategic Measures

Given Organizational Objectives . . .

Measure 1

Percentage of resilience “activities”(*) that *do not* directly (or indirectly) support one or more organizational objectives

Measure 2

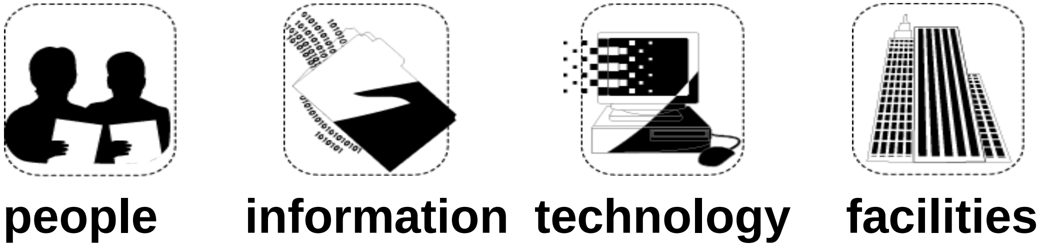
For each resilience “activity,” number of organizational objectives that require it to be satisfied (goal is = or > 1)

(*) “Activity” can be a project, task, performance objective, investment, etc. It represents some meaningful decomposition of the resilience program.

Given High-Value Services and Assets . . .

Measure 3

Percentage of high-value services that *do not* satisfy their allocated resilience requirements(*)



Measure 4

Percentage of high-value assets(+) that *do not* satisfy their allocated resilience requirements(*)

(*) confidentiality, availability, integrity; (+) technology, information, facilities, people

Given Controls . . .

Measure 5

Percentage of high-value services with controls that are ineffective or inadequate

Measure 6

Percentage of high-value assets with controls that are ineffective or inadequate

Given Risks . . .

Measure 7

Confidence factor that risks(*) from all sources that need to be identified have been identified

Measure 8

Percentage of risks with impact above threshold

(*) to high-value assets that could adversely affect the operation and delivery of high-value services

Given a Disruptive Event (*)

Measure 9

Probability of delivered service through a disruptive event

Measure 10

For disrupted, high-value services with a service continuity plan, percentage of services that *did not* deliver service as intended throughout the disruptive event

(*) An incident, a break in service continuity,
a man-made or natural disaster or crisis

Top Ten Strategic Measures

1. Percentage of resilience “activities” that *do not* directly (or indirectly) support one or more organizational objectives

2. For each resilience “activity,” number of organizational objectives that require it to be satisfied (goal is = or > 1)

3. Percentage of high-value *services* that **do not** satisfy their allocated resilience requirements

4. Percentage of high-value *assets* that **do not** satisfy their allocated resilience requirements

5. Percentage of high-value *services* with controls that are ineffective or inadequate

6. Percentage of high-value *assets* with controls that are ineffective or inadequate

7. Confidence factor that risks from all sources that need to be identified have been identified

8. Percentage of risks with impact above threshold

9. Probability of delivered service through a disruptive event

10. For disrupted, high-value services with a service continuity plan, percentage of services that *did not* deliver service as intended throughout the disruptive event

If These Don’t Work For You . . .

Identify the high-level objectives for your resilience program

Define measures that demonstrate the extent to which objectives are (or are not) being met

Make sure the measures you are currently reporting support one or more objectives

Measurement is expensive; collect and report measures that inform decisions and affect behavior

Getting Started

To Get Started

Identify sponsors and key stakeholders

Define resilience objectives and key questions

Determine information and processes that inform these

Define and vet a small number of key measures

Collect, analyze, report, refine

Put a measurement process in place (start small)

References

CERT Podcast: Measuring Operational Resilience
http://www.cert.org/podcast/show/20111004allen.html

[Allen 2011a] Allen, Julia; Curtis, Pamela; Gates, Linda. *Using Defined Processes as a Context for Resilience Measures* (CMU/SEI-2011-TN-029). Software Engineering Institute, Carnegie Mellon University, October 2011. (forthcoming)

[Allen 2011b] Allen, Julia & Curtis, Pamela. *Measures for Managing Operational Resilience* (CMU/SEI-2011-TR-019). Software Engineering Institute, Carnegie Mellon University, June 2011. http://www.sei.cmu.edu/library/abstracts/reports/11tr019.cfm

[Allen 2010] Allen, Julia & Davis, Noopur. *Measuring Operational Resilience Using the CERT Resilience Management Model* (CMU/SEI-2010-TN-030). Software Engineering Institute, Carnegie Mellon University, September 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tn030.cfm

[Caralli 2010] Caralli, Richard A.; Allen, Julia H.; White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2010.

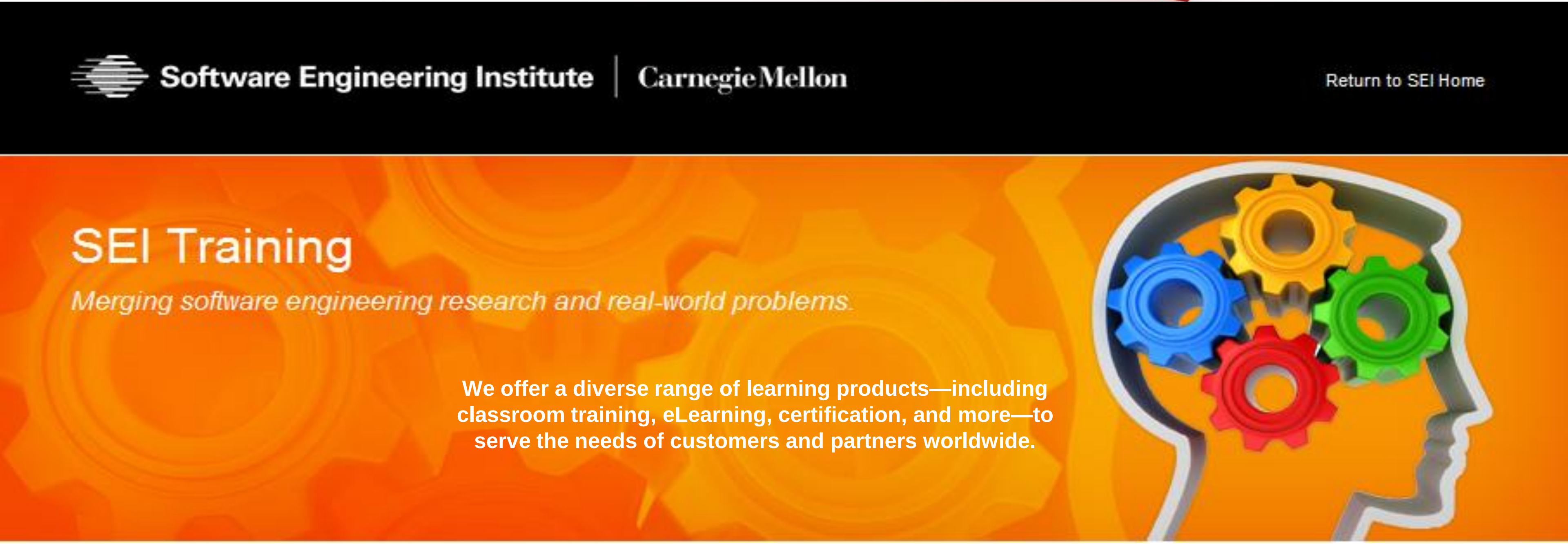
[Hubbard 2010] Hubbard, Douglas. *How to Measure Anything*. John Wiley & Sons, 2007.

visual-literacy.org. “A Periodic Table of Visualization Methods.”
http://www.visual-literacy.org/periodic_table/periodic_table.html

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE 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 work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.



SEI Training

Merging software engineering research and real-world problems.

We offer a diverse range of learning products—including classroom training, eLearning, certification, and more—to serve the needs of customers and partners worldwide.