Applying CERT-RMM: Users Group Workshop Experiences

12th Annual CMMI Technology Conference and User Group

Julia Allen; Software Engineering Institute/CERT Program
Lynn Penn; Lockheed Martin IS&GS

7 November 2012

Topics

CERT Resilience Management Model (CERT-RMM) overview

CERT-RMM Users Group overview

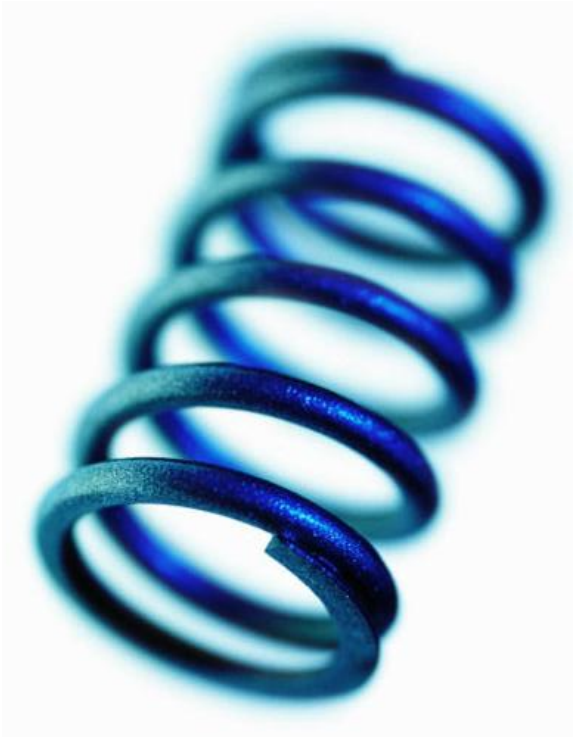
Member reports

- Discover Financial Services
- US Postal Inspection Service
- Carnegie Mellon University Information Security Office
- CERT Resilience Enterprise Management Team
- Lockheed Martin IS&GS (in depth)

CERT-RMM Overview

Operational resilience defined

Resilience: The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit
[wordnet.princeton.edu]



Operational resilience: The ***emergent*** property of an ***organization*** that can ***continue to carry out its mission*** in the presence of ***operational stress*** and ***disruption*** that ***does not exceed*** its limit
[CERT-RMM]

Where does the **stress** and **disruption** come from? Risk.

Operational resilience and operational risk

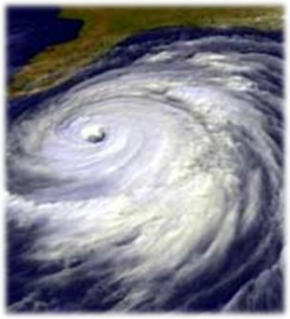
Operational resilience emerges from effective **operational risk management**

Operational risk categories:

Actions of people

Systems and technology failures

Failed internal processes



External events

What is CERT®-RMM?

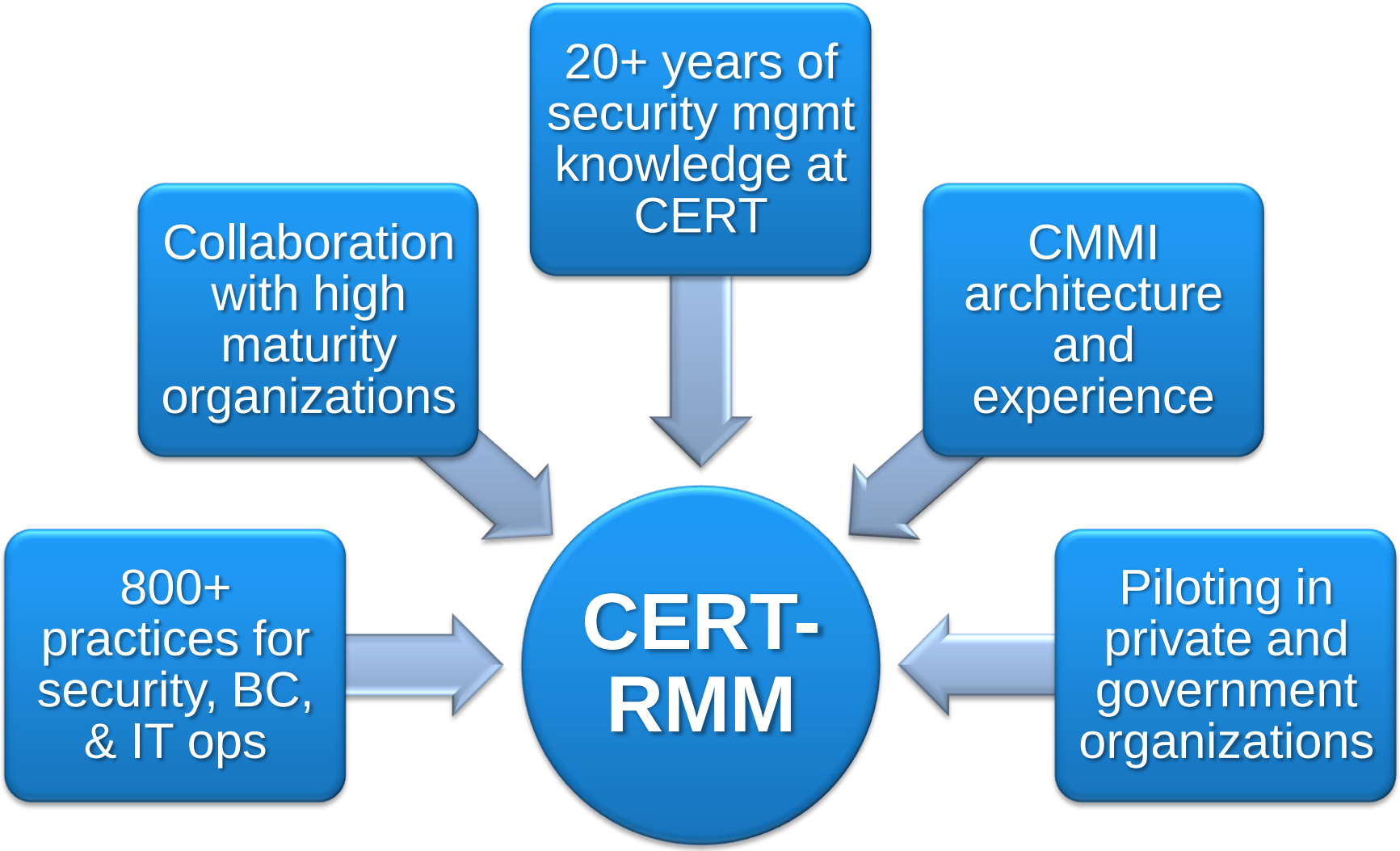
CERT-RMM is a capability model for managing and improving operational resilience.

"…an extensive super-set of the things an organization could do to be more resilient."

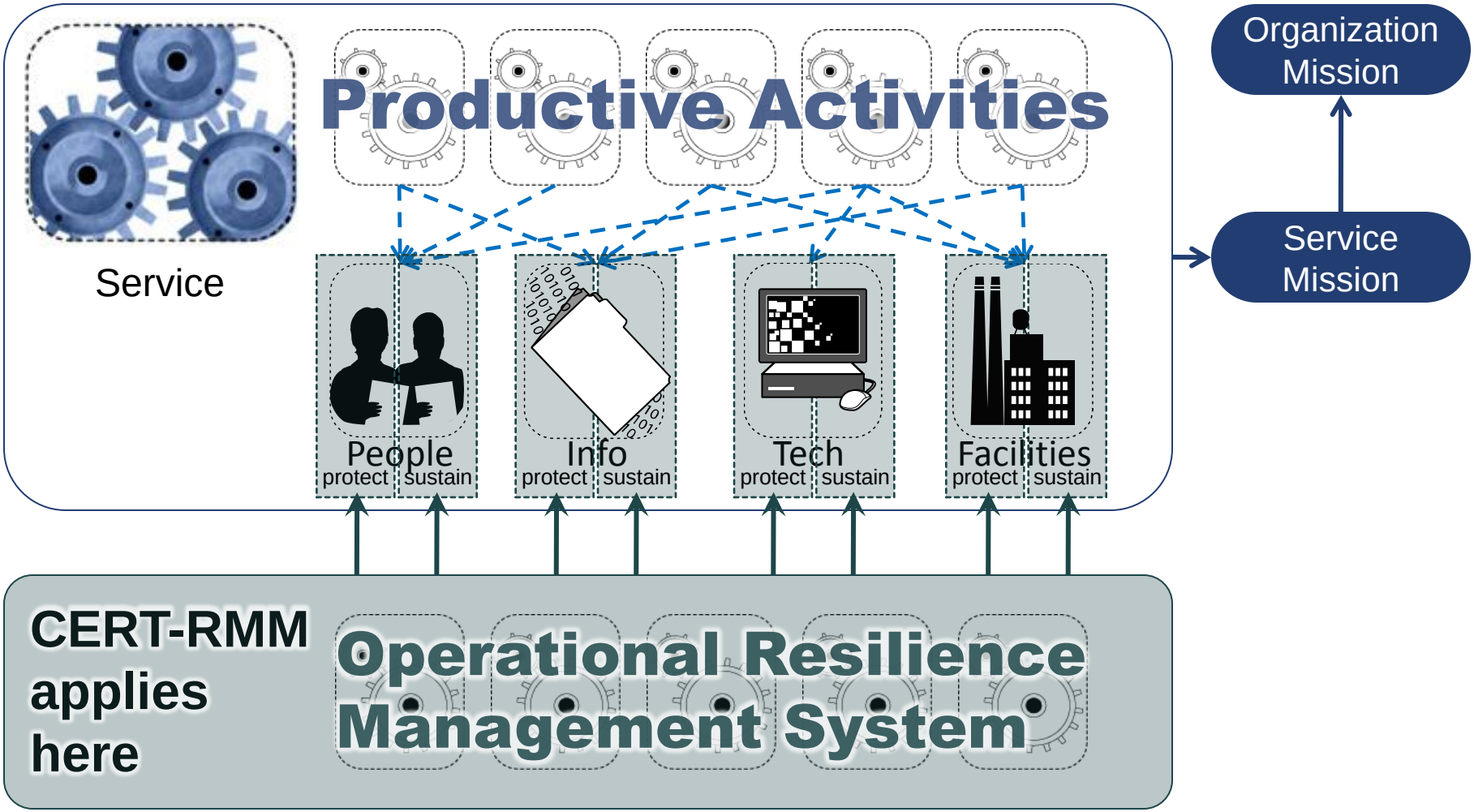
- CERT-RMM adopter

- 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 *(like CMMI)*
- Enables measurement
- Improves confidence in how an organization responds in times of operational stress

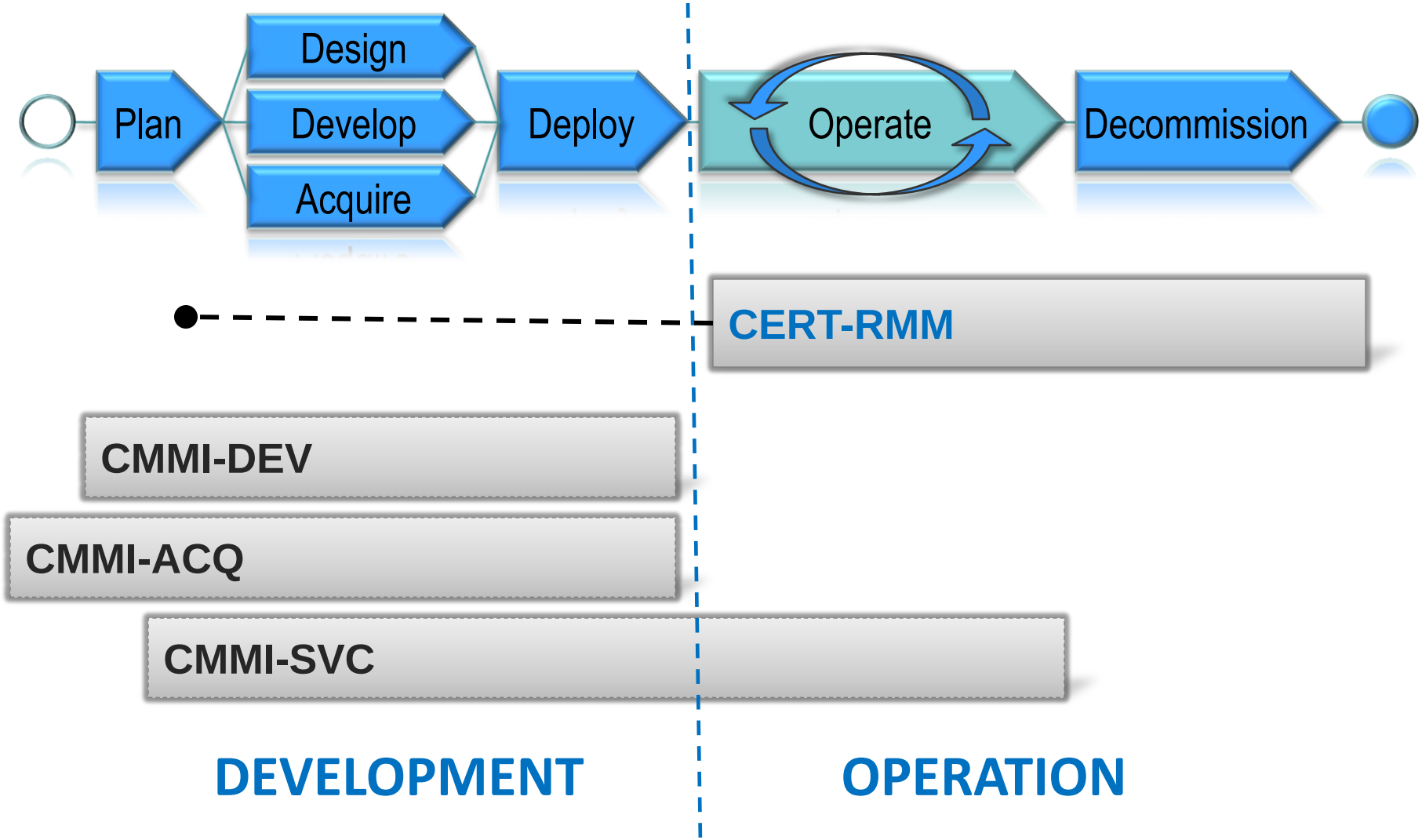
CERT-RMM background



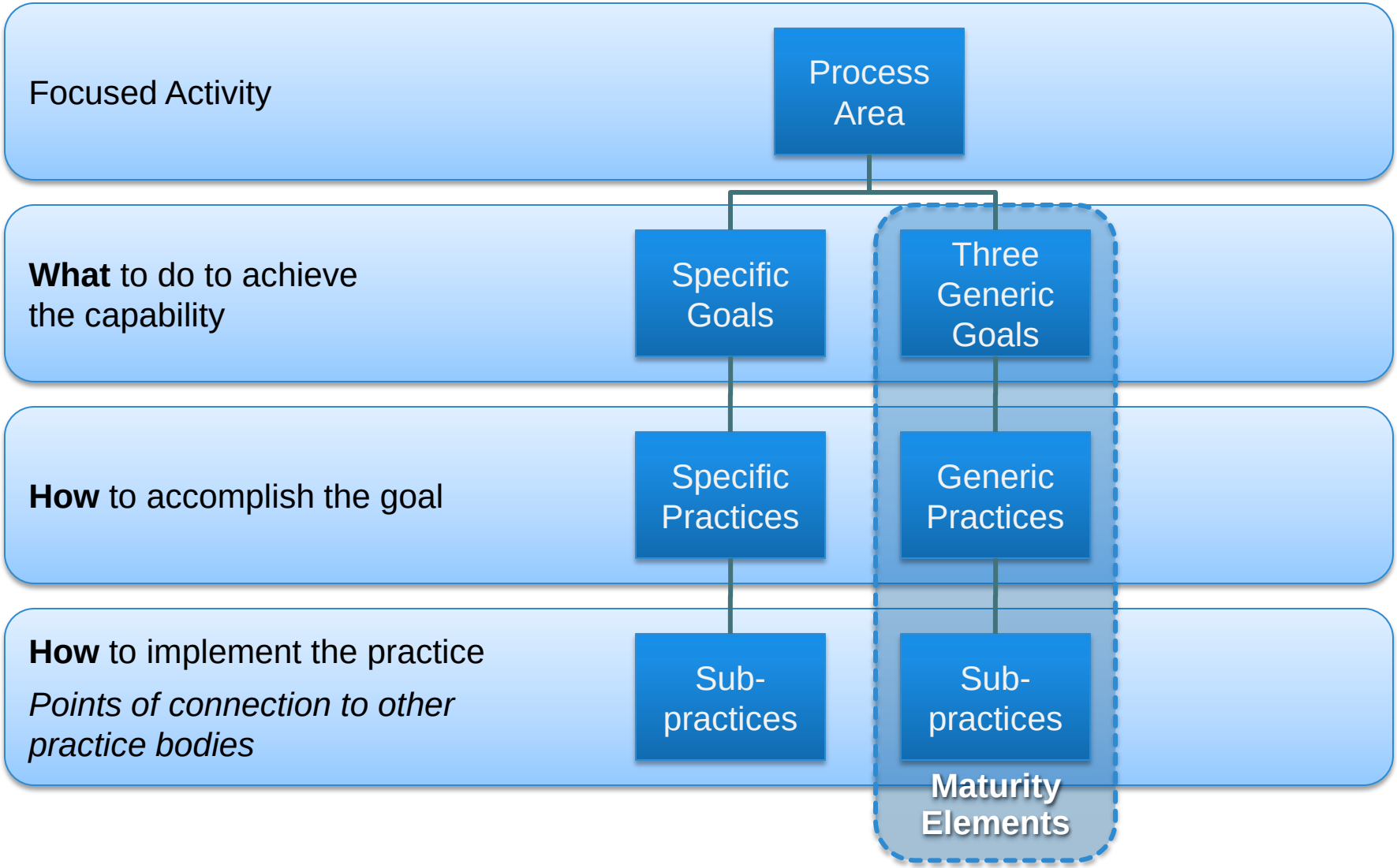
Distinguishing resilience processes



For comparison: CERT-RMM & CMMI



CERT-RMM process area architecture



CERT-RMM: 26 process areas in 4 categories

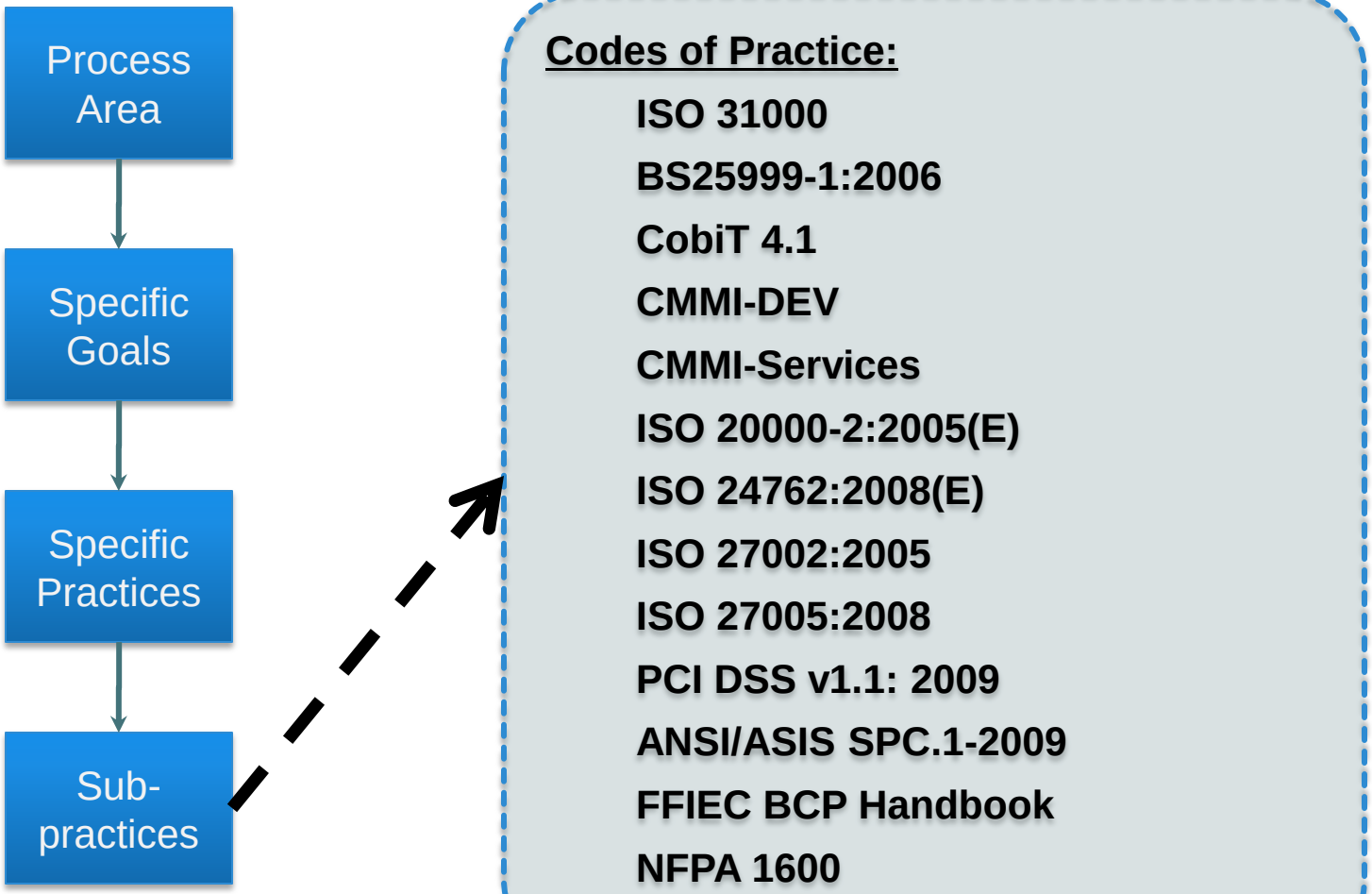
Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

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 Management
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

CERT-RMM Links to Codes of Practice (2011)



CERT-RMM numbers

4
Categories

26
Process Areas

94
Specific Goals

251
Specific Practices

3
Generic Goals
per process area

13
Generic Practices
per process area

Where to start

To use the model, start by selecting any number of process areas (or even parts of process areas) that align with your objectives.

Starting with 1 process area or a few specific goals is completely acceptable.

There is no requirement to use the entire model—**use whatever parts of the model make sense for your situation.**

CERT-RMM Users Group (RUG) Overview

RUG objectives

Engage in customized collaborative discussions, hands-on activities, and workshops to:

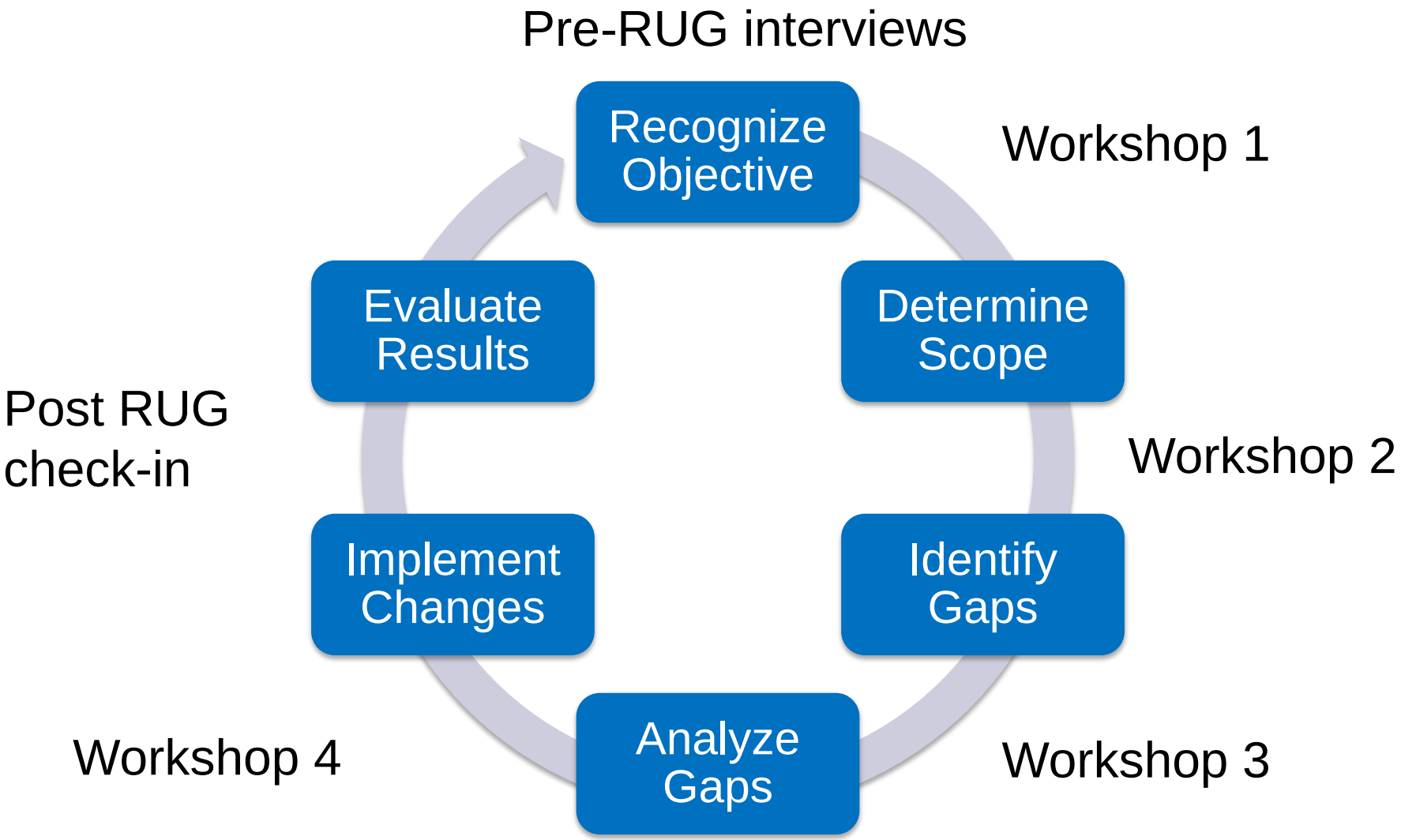
- implement a solution that meets a specific resilience improvement objective tied to an organizational goal
- improve the effectiveness and efficiency of operational risk management activities
- diagnose their current resilience activities against CERT-RMM processes and practices
- conduct peer-to-peer comparisons and learn from others, including CERT-RMM developers and appraisers
- define processes and identify measures to evaluate and improve resilience
- learn how to reduce the complexity and improve the efficiency of compliance and other assessment-related activities

RUG structure

Four 2-day workshops conducted over 10-12 months; conference calls in between workshops

Members identify needs and objectives for their specific workshop series in advance

RUG “Architecture”



Member Reports

US Postal Inspection Service

CERT-RMM Users Group

Organization

- U.S. Postal Inspection Service (USPIS) - one of two law enforcement arms of the US Postal Service (USPS).
- USPS-Office of Inspector General - responsible for all internal crimes within the USPS.
- USPIS - responsible for protecting the security of the USPS brand name, facilities, information and technical assets.
- USPIS enforces over 200 federal statues - electronic crimes, mail fraud, mail theft, identity theft, child exploitation and prohibited mailings such as bombs, biological and chemical threats.
- USPIS Revenue & Product Security group (members of the CERT-RMM Users Group) specifically investigates external computer security incidents targeted at USPS and its customers and makes recommendations to USPS-IT for information security improvements.
- USPS-IT has ultimate decision to accept or reject recommendations.

How USPIS used CERT-RMM

- CERT-RMM assisted USPIS to improve processes within computer incident response and management.
- Enhanced communication with relevant internal stakeholders and assisted in defining and enhancing incident response, specifically:
  - Identification
  - Containment
  - Eradication
  - Recovery
- USPIS recommended additional policies added to existing USPS-IT security policies to incorporate law enforcement functions.
- USPIS created and recommended use of a more profound computer incident handling guide similar to NIST and CERT to improve effectiveness of response to a computer-related incident.

Value of CERT-RMM

- Network with other academia, private, and governmental organizations.
- Immediate access to knowledgeable CERT-RMM instructors who provided valuable feedback to project improvement.
- Access to various types of documents and templates to assist with narrowing project scope, processes, and procedures.

Carnegie Mellon University
Information Security Office

Carnegie Mellon University

Carnegie Mellon

- Est 1967 in Pittsburgh, PA
- Global, private research university
- Ranked 22nd
- 15,000 faculty, staff, students
  - 4,000 faculty and staff
  - 11,000 students
  - 84,000 alumni
- Entrepreneurial, highly distributed, ‘scrappy’

Our RMM Journey

Carnegie Mellon

"I'd been searching for tools and techniques to conduct security risk assessments and to evaluate and improve the capability of our information security program. While pursuing the first, via OCTAVE Allegro training, I became aware of CERT-RMM.

The notion of "resilience" better characterized what our information security program is really about. Further, I saw it as a potential unifying theme for my partners in DR/BC and operations. It explained how our areas of focus interplay to deliver business value.

We exercised the model first within our own incident response function and realized immediate value. The next step was to test it on a more complex improvement goal that crossed process areas. Participation in the RUG facilitated this exercise, showed us the gaps in original thinking, and kept us on track."

Mary Ann Blair

Director of Information Security

- Apr 2010 – OCTAVE Allegro training
- Oct 2010 – Intro to RMM training
- Nov 2010 – Pilot discussions begin
- Jan 2011 – Compass assessment of Incident Management and Control (IMC) process area begins
- April 2011 - Compass results guide IMC improvement definition
- Apr 2011- RUG invite accepted
- June 2011- February 2012 - RUG participation guides complex, inter-process area improvement effort

RUG value proposition

Carnegie Mellon

1. Access to the CERT-RMM experts and discussion amongst members greatly improved our objective scope and understanding of the model.
2. Reviewing and tracking others' progress allowed us to apply and test our model understanding on several other use cases. This gave us lots of additional practice without lots of extra effort.
3. We expanded our professional network beyond our usual types of contacts. This made not only the RUG sessions a more interesting experience but gave us a richer set of professional contacts to share with in the future.
4. The trust we established, and frankly required, allowed us to dig deep into a wide set of issues that can help a project succeed or lead a project to failure. The detours we took were as valuable as the set agenda.
5. Contributing directly to the improvement of the model and supporting materials was a personally rewarding by-product of RUG participation.

CERT Resilience Enterprise Management Team

REM overview

CERT Resilience Enterprise Management team responsible for CERT-RMM:

- development and transition
- training
- appraisals
- users group
- licensing and certification
- application and tailoring of the model for customer engagements

Use of CERT-RMM

Improvement objective: Protect and sustain customer data in accordance with customer requirements (collect, develop, serve as custodian for)

Model scope: ADM, KIM, RRD

Results to date

- Customer data handling process definition
- Specific customer data procedure definitions
- Information asset profiles
- Defined measures
- Process asset repository
- Stakeholder buy-in

Value of the RUG

Formalized and documented a key operational process

Better understanding of all aspects of a CERT-RMM process improvement project

Incentivized to develop example artifacts in advance, to assist RUG members with their projects

Developed effort estimates for each improvement project phase

Obtained valuable improvement suggestions for subsequent RUG workshops (case studies, more prescriptive guidance early on)

LOCKHEED MARTIN

Stealth Integration of CERT® Resilience Management Model

Lockheed Martin Corporation
Integrated Systems and Global Solutions

Lynn Penn
Director Strategic Process Engineering

November 2012

RMM Adoption Considerations

- RMM Alignment with Business Strategies and Objectives
- RMM Integration into current processes
- RMM Integration into current business rhythms
- RMM Performance measurement

LOCKHEED MARTIN

Improvement Objective

- Objective: Pilot selected RMM practices to show value in meeting LM IS&GS strategic objectives

But **what** strategic objectives?

Improvement Objectives

Driver / Pain Point	Initiative	Assessment	Stealth Possibility?	Positives	Negatives	Project Decision / Priority	Additional tasks needed in order to make decision
Driver: CTO "Continue Cyber Security Path to Excellence"	Use Crosswalk to create a CALiPER view	Possible	Yes	1. Future applicability if adopt model 2. No additional involvement outside SPE 3. Will provide gap analysis	A. Not very visible to organization B. Not a true use of the model C. No real benefit D. Scope goes beyond true use of CALiPER	Possible	None
Driver: CTO "Continue Cyber Security Path to Excellence"	Establish Organizational processes and process assets	Long term possibility	Yes	1. Would move all of IS&GS into compliance 2. Partially in line with Performance Analytics activities 3. Could start with a policy review for intent (same as EBS did for DR, COOP, CM, and PP)	1. Would require support from multiple functions and product lines 2. Difficult to determine where to begin	Possible	1. Buy in from PAL Consolidation team.
Driver: CTO "Continue Cyber Security Path to Excellence"	Enterprise Risk Management to include resiliency risks	Very Difficult	No	1. Increased visibility on resiliency issues 2. IS&GS-level activity 3. Can start "small" by introducing resiliency issues into the checklists of questions asked for Cyber programs only 4. Could use questions from	1. Difficult to get buy-in from organization currently leading effort (maybe) 2. Extensive training may be required 3. Where to begin?	Possible	1. Determine interest - buy in from either Programs or a product line 2. Get PAR schedule from product line
Driver: CTO "Continue Cyber Security Path to Excellence"	Cloud Computing Roadmap	Very Difficult	No	1. Roadmap provided in book 2. Covers several process areas 3. Cloud Computing is a strategic Initiative 4. Cloud Computing a separate initiative	1. Cloud computing focused under one person, but updates would have to be spread across several organizational functions	Possible - probably hardest	1. Determine interest - buy in from CTO/ buy in from CC Initiative

- 15 possibilities, from “Possible” to “Very Difficult”
  - Difficult when multiple internal groups had to coordinate
  - Possible when “pain” was localized

RMM Content

- IS&GS took a look at the Process Areas/ Goals / Practices within RMM to identify what concepts were appropriate.
  - Full model scope would be difficult (26 PAs, 94 SGs, 251 SPs)
  - Often an entire Process Area was not applicable, therefore going down to the Goals and associated practices was needed.

But **what** Process Areas should we consider?

LOCKHEED MARTIN

RMM Content (2)

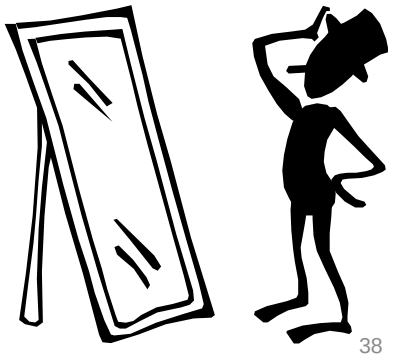
- Given the Improvement Objectives, most likely PAs were:
  - Engineering Process Areas:
    - Resilience Requirements Development (RRD)
    - Resilience Requirements Management (RRM)
    - Resilient Technical Solution Engineering (RTSE)
    - Service Continuity (SC)
  - Enterprise Management Process Areas:
    - Enterprise Focus (EF)
    - Organizational Training and Awareness (OTA)
    - Risk Management (RISK)
  - Operations Process Area:
    - External Dependencies Management (EXD)
  - Process Management Process Areas:
    - Organizational Process Definition (OPD)
    - Organizational Process Focus (OPF)

But **how** to implement

- And **how** do you do that with limited authority and budget?

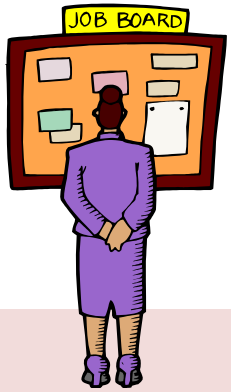
- **Where** can we start?

- Of course, we know **who** has to do this



Final Criteria for Selection

- Minimize impact to organization
- Look for opportunities to insert concepts
  - Integrate into what was already being done
  - Optimize existing Business Rhythm
- Look for opportunities to find the "state of the practice"



In other words, be opportunistic!

Final Criteria for Selection

- Added Columns to decision spreadsheet
  - Could we act without creating new activities?
  - Should we pursue?

Driver / Pain Point	Initiative	Assessment	Stealth Possibility?	Positives	Negatives	Project Decision / Priority	Additional tasks needed in order to make decision
Driver: CTO "Continue Cyber Security Path to Excellence"	Use Crosswalk to create a CALiPER view	Possible	Yes	1. Future applicability if adopt model 2. No additional involvement outside SPE 3. Will provide gap analysis	A. Not very visible to organization B. Not a true use of the model C. No real benefit D. Scope goes beyond true use of CALiPER	Possible	None
Driver: CTO "Continue Cyber Security Path to Excellence"	Establish Organizational processes and process assets	Long term possibility	Yes	1. Would move all of IS&GS into compliance 2. Partially in line with Performance Analytics activities 3. Could start with a policy review for intent (same as EBS did for DR, COOP, CM, and PP)	1. Would require support from multiple functions and product lines 2. Difficult to determine where to begin	Possible	1. Buy in from PAL Consolidation team.
Driver: CTO "Continue Cyber Security Path to Excellence"	Enterprise Risk Management to include resiliency risks	Very Difficult	No	1. Increased visibility on resiliency issues 2. IS&GS-level activity 3. Can start "small" by introducing resiliency issues into the checklists of questions asked for Cyber programs only 4. Could use questions from	1. Difficult to get buy-in from organization currently leading effort (maybe) 2. Extensive training may be required 3. Where to begin?	Possible	1. Determine interest - buy in from either Programs or a product line 2. Get PAR schedule from product line
Driver: CTO "Continue Cyber Security Path to Excellence"	Cloud Computing Roadmap	Very Difficult	No	1. Roadmap provided in book 2. Covers several process areas 3. Cloud Computing is a strategic Initiative 4. Cloud Computing a separate initiative	1. Cloud computing focused under one person, but updates would have to be spread across several organizational functions	Possible - probably hardest	1. Determine interest - buy in from CTO/ buy in from CC Initiative

LOCKHEED MARTIN

Possible Projects

- Used all columns (not just “Stealth Possibility”) in determining final set of possibilities.
  - Narrowed to 6 “Possible” projects
  - Then added columns:
    - Organizational Scope
    - Model Scope
    - How we could measure the project?
- Decision made to implement a project where we had the most control
  - No “external” training or buy-in required
  - Use results and lessons learned to identify next projects

LOCKHEED MARTIN

And the Winner was…..

- Add RMM questions in CMMI-DEV SCAMPI Bs to identify gaps:
  - Would be doing at least 5 SCAMPI Bs in preparation for a SCAMPI A
  - Organizational Scope:
    - Strategic Process Engineering
    - Selected programs within one product line (potentially a second product line)
- Model Scope:
    - RRD:SG2.SP1 and RRD:SG3.SP1 – add questions to CMMI-DEV RD
    - RRM:SG1.SP1-4 – add questions to CMMI-DEV REQM
    - RTSE:SG1.SP3, SP4 – add questions to CMMI-DEV TS
    - EXD:SG3.SP2 – add question to CMMI-DEV SAM
    - RISK:SG1.SP1 and RISK:SG3 – add questions to CMMI-DEV RSKM

LOCKHEED MARTIN

Purpose of Project

- See whether it is possible to blend (harmonize) several assessments (i.e., RMM and SCAMPI B or RMM and Internal ISO Audits)
- See if there are any systemic program issues we should address
  - If there are, could we do a root cause analysis on the issues or would we need additional information?
- Report the findings to Chief Technology Officer and Senior Management associated with our Cyber Security activities
- Report results to the RMM User Group

LOCKHEED MARTIN

Diagnostics to be Used

- No new diagnostics needed
- Identified RMM-related questions and added them to current diagnostics in use for SCAMPI Bs
  - Supplemented by questions to the B/C Team Leads
- Would analyze results two ways:
  - Could this method be used in IS&GS?
  - Are there issues that need to be surfaced to management based on the answers to the RMM questions

Example of Questions Added

- Added to Supplier Agreement Management (SAM)

2	Shared	SAM	**SP 1.3 Establish and maintain supplier agreements.**	
2	Shared	SAM	1. How are agreements with suppliers established and maintained?	
	RMM	EXD	2. Do the agreements with suppliers include specifications that relate to resilience, like availability, business continuity, performance, response time, security, etc? [EXD:SG3.SP2]	

Example of Questions Added

- Added to Requirements Development (RD)

DEV	RD	**SP 1.1 Elicit stakeholder needs, expectations, constraints, and interfaces for all phases of the product life cycle.**	
DEV	RD	1. How do you engage relevant stakeholders using methods for eliciting needs, expectations, constraints, and external interfaces?	
RMM	RRD	2. Do you have different methods for engaging customers to elicit needs for things like data integrity, availability, security, etc.?	

DEV	RD	**SP 2.1 Establish and maintain product and product component requirements, which are based on the customer requirements.**	
DEV	RD	1. How do you develop requirements in technical terms necessary for product and product component design?	
DEV	RD	2. How do you derive requirements that result from design decisions? Can you give any examples?	
RMM	RRD	3. How are protection, cyber-security, data integrity, availability, and business continuity requirements identified and derived? Can you give any examples? [RRD:SG2.SP1]	

AND THE RESULTS WERE

Example Analysis of Results – RMM Questions

- From SAM:

2	Shared	SAM	**SP 1.3 Establish and maintain supplier agreements.**	
2	Shared	SAM	1. How are agreements with suppliers established and maintained?	
	RMM	EXD	2. Do the agreements with suppliers include specifications that relate to resilience, like availability, business continuity, performance, response time, security, etc? [EXD:SG3.SP2]	P1: Suppliers mostly provide people - and they have to have certain security clearances and security-related knowledge and security-related certifications; requirements are flowed down to subs. P2: NA

Example Analysis of Results – RMM Questions

- From RD:

DEV	RD	**SP 1.1 Elicit stakeholder needs, expectations, constraints, and interfaces for all phases of the product life cycle.**	
DEV	RD	1. How do you engage relevant stakeholders using methods for eliciting needs, expectations, constraints, and external interfaces?	
RMM	RRD	2. Do you have different methods for engaging customers to elicit needs for things like data integrity, availability, security, etc.?	P1: Same TIM, but with different people; separate IA meetings for accreditation process. P2: Mapping of responsibilities of system and inherited many of the controls from prime. In deployed system the responsibilities are diverse as far as DIACAP and Resilience for operation and environment. Most of these were process and environment. SOSCO put in all the encryption.

DEV	**RD**	**SP 2.1 Establish and maintain product and product component requirements, which are based on the customer requirements.**	
DEV	**RD**	1. How do you develop requirements in technical terms necessary for product and product component design?	
DEV	**RD**	2. How do you derive requirements that result from design decisions? Can you give any examples?	
RMM	**RRD**	3. How are protection, cyber-security, data integrity, availability, and business continuity requirements identified and derived? Can you give any examples? [RRD:SG2.SP1]	P1: Guidelines from SOP; design packages include everything, including these type of requirements. P2: See above

LOCKHEED MARTIN

Status

- Current:
  - Number of issues found with RMM questions – No significant issues
  - Number of "opportunities" to gather data – 8
  - Number of RMM practices incorporated into SCAMPI questions - 14
  - Number of changes needed to SCAMPI B process in order to ask RMM questions - 9
- Future:
  - Number of RMM practices incorporated into Internal ISO Audits
  - Number of changes needed to Internal ISO Audit process in order to ask RMM questions

LOCKHEED MARTIN

Can This Method be Used In IS&GS?

Yes, this method can be used in IS&GS!

- May want to consider adding questions to additional reviews / assessments in the business rhythm
  - Design Adequacy Assessments
  - Internal ISO 27001 Audits
  - Program Performance Reviews
- May need to ensure additional people are being interviewed
  - As follow-up interviews as needed
- Will have to ask for additional evidence for SCAMPI Bs

LOCKHEED MARTIN

Are there issues that need to be surfaced to management based on the answers to the RMM questions? - 1

- Engineering – No issues to surface to management
  - Resilience Requirements Development (RRD): Development program resilience requirements are elicited from the customer and/or derived from additional analysis and required functionality is established
  - Resilience Requirements Management (RRM): Once requirements have been identified, they are managed like any other requirement
  - Resilience Technical Solution Engineering (RTSE): Most programs have guidelines for designing and implementing resilience into software and systems (or use commercial guidelines);

LOCKHEED MARTIN

Are there issues that need to be surfaced to management based on the answers to the RMM questions? – 2

- Risk Management (RISK) – No issues to surface to management
  - Risk sources include resilience issues; no separate categories established, but resilience risks are included in established categories (typically: cost, schedule, technical, programmatic)
  - Risks identified to both assets and services

Comment: The larger issue of Risk Tolerance was not addressed in questions

LOCKHEED MARTIN

Are there issues that need to be surfaced to management based on the answers to the RMM questions? - 3

- External Dependencies Management (EXD) – No issues to surface to management
  - Supplier Agreements can include resilience requirements
    - If identified as needed by Engineering or Program Management

Comment: No issues, but more general awareness is needed in Global Supply Chain Management and Contracts organizations

LOCKHEED MARTIN

Questions?

Contact Information

- Lynn Penn: mary.lynn.penn@lmco.com
- Dorna Witkowski: dorna.witkowski@lmco.com

© 2011 Lockheed Martin Corporation. All rights reserved.

Socializing CERT-RMM

- Choose an organizational and model scope that you can control - go narrow and be specific
- Understand cultural norms for introducing a new idea
- Understand business rhythm: capitalize on current initiatives
- Use organizational terms and language: “Put the RMM book in the drawer”
- Extend current diagnostic methods
- Keep your sponsor in mind: WIIFM (What’s In It For Me)

Resources - 1

Training

Introduction to the CERT Resilience Management Model (3-day course)

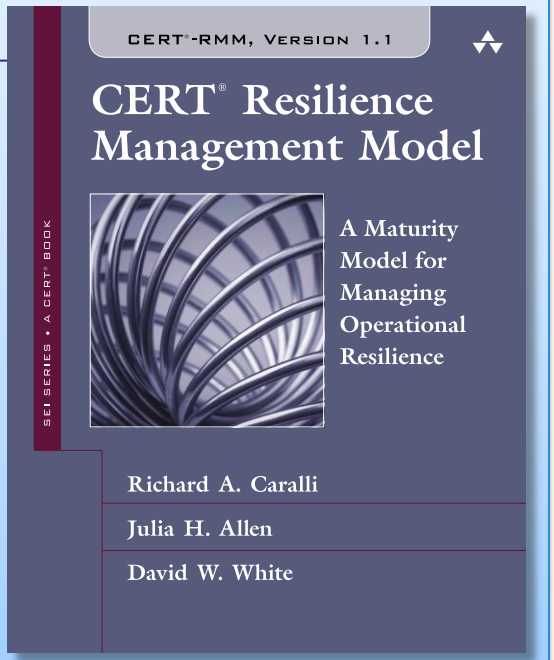
- Public courses
- Private onsite courses by arrangement

www.sei.cmu.edu/training/P66.cfm

Lead appraiser apprenticeship program is also available to certify people in leading CERT-RMM-based appraisals

Book

Includes full model (v1.1) plus adoption guidance and perspectives from real-world use of the model.



Available at Amazon.com

www.cert.org/resilience

email: info@sei.cmu.edu

Resources – 2

Allen, Julia & Young, Lisa. *Report from the First CERT-RMM Users Group Workshop Series* (CMU/SEI-2012-TN-008). Carnegie Mellon University: Software Engineering Institute, April 2012. http://www.sei.cmu.edu/library/abstracts/reports/12tn008.cfm

Caralli, Richard A.; Allen, Julia H.; White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011.

CERT-RMM Users Group Workshop Series: http://www.sei.cmu.edu/training/P92.cfm

CERT-RMM website: http://www.cert.org/resilience/rmm.html

CERT-RMM Measurement & Analysis website: http://www.cert.org/resilience/rma.html

CERT Podcast Series: Security for Business Leaders, specifically podcasts on risk management & resilience: http://www.cert.org/podcast/

Contact Information

- Julia Allen, CMU/SEI/CERT: jha@sei.cmu.edu
- Lynn Penn; Lockheed Martin IS&GS: mary.lynn.penn@lmco.com

Software Engineering Institute | Carnegie Mellon