Software Engineering Institute

LOCKHEED MARTIN

Application of the CERT® Resilience Management Model at Lockheed Martin

March 2011

David White
Carnegie Mellon University Software Engineering Institute
dwhite@cert.org

Dr. Nader Mehravari
Executive VP, IT Cadre
SEI Affiliate
nader.mehravari@ITCadre.com

William David
Lockheed Martin Enterprise Business Services
william.david@lmco.com

Abstract

- Lockheed Martin Corporation has collaborated with the Software Engineering Institute on the application of the CERT© Resilience Management Model (CERT-RMM) to improve Lockheed Martin's corporate-wide business continuity, IT disaster recovery, crisis management, and pandemic planning activities. Two CERT-RMM Class C appraisals have been conducted as part of the collaboration. This presentation will provide an overview of the project, information about the appraisals, and a summary of the use of the appraisal results.

Contents

- The need for a common assessment model
- Resiliency Management Model (RMM)
- Two Trials at Lockheed Martin
  - December 2009
  - August 2010
- Observations from August 2010 Assessment of LM Command Media Related to Business Resiliency

Definition of Business Resiliency

- Business Resiliency Management (BRM) is the practice of planning, developing, executing, and governing activities to ensure that an enterprise:
  - Identifies and mitigates operational risks that can lead to business disruptions before they occur,
  - Prepares for and responds to disruptive events (natural or man-made, accidental or intentional) in a manner that demonstrates command and control of incident response,
  - Recovers and restores mission-critical business operations following a disaster within acceptable time frames.

Business Resiliency Initiative at Lockheed Martin

- Corporate-wide strategic program intended to holistically look at principles, practices, tools, and technologies being used across the corporation for preparedness planning

- Scope of the Initiative
  - IT Disaster Recovery (DR)
  - Business Continuity (BC)
  - Pandemic Planning (PP)
  - Workforce Continuity (WC)
  - Crisis Management (CM)
  - Emergency Management (EM)

- The initiative has established a strategic framework and operational practices to continually improve the corporation's resilience to disruption or loss in supplying its products and services.

One of the Business Problems Addressed

- Observations and Shortcomings
  - Inconsistent and unrepeatable assessment of business entities' DR and BC posture due to lack of a common assessment/measurement mechanism
    - No common ruler
    - No maturity model
  - Lack of continuous monitoring of business entities' and/or the Corporation's DR and BC posture
  - Lack of a common mechanism to establish improvement goals, measurements criteria, and tracking
  - Inconsistent and unrepeatable self assessments by business entities of their current DR and BC posture
  - Lack of continuous self assessment by business entities

There is a Need for Common Ruler for Business Resiliency Assessment

Applications of an Enterprise-Wide Common Ruler
(a.k.a. Maturity Model)

- To assess current level of competencies
  - Where are we now? How good are we now?
  - A consistent and common "ruler"
  - Assessment by: self, internal 3rd party, external 3rd party
- To guide future direction and investments
  - Where do we want to be? How well do we want to get?
  - Setting objectives
  - Determining the investments required to reach the next/desired level
  - Not necessary for all organizations to reach the most top level
- To measure progress towards the desired goal
- Once the desired level is reached, to ensure that the plans and processes continue to evolve with the needs of the organization
  - How do we stay there?

Approach

- Step 1
  - Environmental scan to identify existing maturity models
- Step 2
  - Comparative trade study of existing maturity models
- Step 3
  - Selecting a candidate maturity model
- Step 4
  - Trial and evaluation
- Step 5
  - Confirming the selection
- Step 6
  - Putting it into regular practice

Trade Study Criteria

- Applicability to Corporation's business model
- Completeness and comprehensiveness of the framework
- Expandability beyond its current scope
- Ease of customization
- Integrated approach to components of business resiliency
- Applicability to other operations processes than business resiliency
- Openness of the framework
- Consistency with national and/or international standards
- Availability of variety of assessment methodologies
- Availability of full documentation
- Availability of training material
- Addressing the complete range of assets
- Addressing governance and management structures
- Familiarity of the model to other management/maturity models being used for other purposes
- Use by other industries of interest

Results of the Trade Study

- RMM was identified as the most promising model for use within LM

- Some of the characteristics that set RMM apart from others
  - It promotes the convergence of information security, business continuity, and IT operations
  - Its model of an enterprise matches large corporations like LM
  - Strong risk management approach
  - Its capability to consider risks associated with the protection of assets and risk associated with the sustainment of assets
  - Treating resiliency activities as yet another class of business processes intended to manage operational risks
  - Focusing on measuring and institutionalizing the resiliency processes
  - Having captured best practices from the financial industry which is known for their high quality and effective resiliency practices

CERT® Resilience Management Model (RRM)

- Is a process improvement model for managing operational resiliency
- It promotes the convergence of information security, business continuity, and IT operations activities as a means to actively direct, control, and manage operational resiliency and risk
- Defined by CMU SEI
- Consistent with BS-25999 standard
- Focuses on "what" not "how"
- Common vernacular and basis for planning, communicating, and evaluating improvements
- Provides guidelines and practices for:
  - Implementing, managing, and sustaining operational resiliency activities
  - Managing operational risk through process
  - Measuring and institutionalizing the resiliency process
- For more information see:
  - http://www.cert.org/resilience/

Objective of Recent Trial Activities

- Evaluate the applicability and utility of the RMM for use at Lockheed Martin
  - How well does RMM align with Lockheed Martin's business model and operational practices?
  - Would the use of RMM benefit attainment and maintenance of Lockheed Martin's business continuity and disaster recovery readiness posture?
  - What appraisal methods are efficient and economical enough for utilization along with RMM?

Trial and Evaluation Approach

- 2-Step Process
- Step 1 – December 2009
  - Limited to disaster recovery preparedness planning
  - Limited to corporate command media for disaster recovery
  - Limited to practices in one of the business units of the Corporation
  - Limited number of RMM practices
- Step 2 – August 2010
  - Scope: Corporate command media related to Business Resiliency
    - Draft new disaster recovery policy
    - Business Continuity corporate policy
    - Pandemic Planning corporate guidelines
    - Crisis Management corporate policy
  - Expanded number of RMM practices

Objectives of December 2009 Trial in Owego

- To determine if the use of the RMM would benefit attainment and maintenance of Lockheed Martin's disaster recovery readiness
- To understand lessons learned from use of the RMM in an organization that is a defense contractor that has attained CMMI Maturity Level 5
- To determine whether the use of a SCAMPI C appraisal using RMM would be useful for evaluating Lockheed Martin's disaster recovery readiness.
- To identify improvements to the RMM

Results from December 2009 Trial in Owego

- Trial was successfully completed with objectives met or exceeded
  - Captured both strengths and shortcomings within Owego's IT DR practices
  - Revealed insights about LM DR Command Media IPM-110

- Summary Results
  - RMM framework appears to be well suited for use within LM
  - For self-assessment needs: Best to use a lightweight appraisal method
  - For assessment of command media: Best to use a SCAMPI-like method

Objectives of August 2010 Trial

- Expand upon the December 2009 trial
  - Expand functional scope to all aspects of Business Resiliency
  - Expand number of RMM practices
- Evaluate Lockheed Martin corporate-level command media related to business resiliency to determine whether such command media would produce the desired CERT-RMM practices.
- Provide immediate feedback on the new draft DR command media in advance of its planned deployment later in 2010.
- Provide feedback on the existing BC command media to help with improvement efforts for such command media planned for 2011
- Facilitate the development of an overall BR command media roadmap

Potentials for Future Actions

- RMM contributing to our common business resiliency taxonomy and nomenclature
- RMM serving as a contributing reference model for our integrated business resiliency framework
- RMM serving as maturity model to gauge the preparedness posture of individual business entities and/or the Enterprise as a whole in the areas of disaster recovery and business continuity
- RMM serving as a mechanism to reveal insights about existing policies and guidelines
- RMM serving as a guiding tool in the developing of new command media
- RMM serving as a means to communicate key harmonization and convergence across business resiliency and information security

Questions and Discussion

Business Resiliency

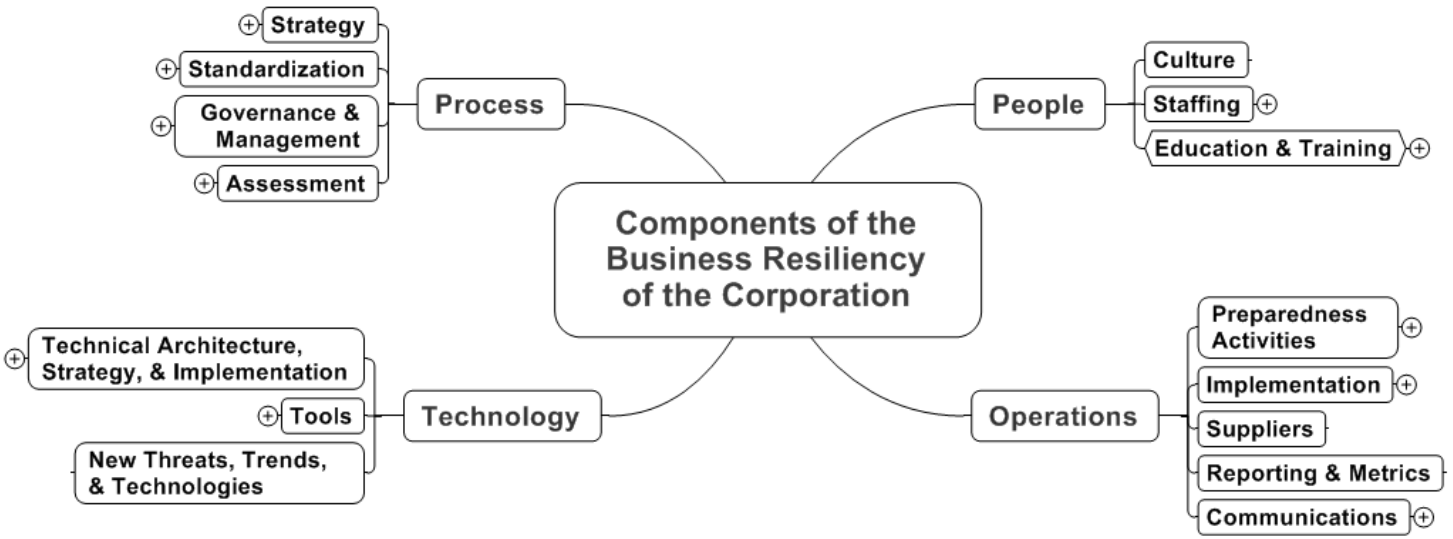
Protecting our people, Sustaining our operations, Safeguarding our assets

Additional Material

Review

- What do we need?
  - A standard scale to measure our progress on improving Lockheed Martin's Business Resiliency posture
  - Ability to measure ourselves against our peers and across the world
  - LM DR/BC Maturity Model

- What is important for us to measure?



Competencies - Review

Important High-Level Competencies:

- **Process**
  - Develop a comprehensive strategy for DR/BC and related components
  - Standardize our DR/BC processes with industry and government standards
  - Form a governance model
  - Utilize continuous analysis models for measuring improvement
- **Technology**
  - Form depth in DR/BC technology
  - Utilize common tools to gather and share DR/BC data
  - Become aware of new DR/BC threats and the technologies to mitigate them
- **People**
  - Create a culture of understanding for DR/BC readiness importance
  - Utilize dedicated staff for DR/BC
  - Create a skill center to train personnel in the field
- **Operations**
  - Create and maintain necessary DR/BC documentation (Plans, Ratings, Risk Assessments)
  - Determine if DR/BC plan success rate and document improvements for the future
  - Ensure a plan is in place to communicate progress (through defined metrics) and best practices to the organization

Recommendation

- Utilize a LM focused **Resiliency Maturity Model**

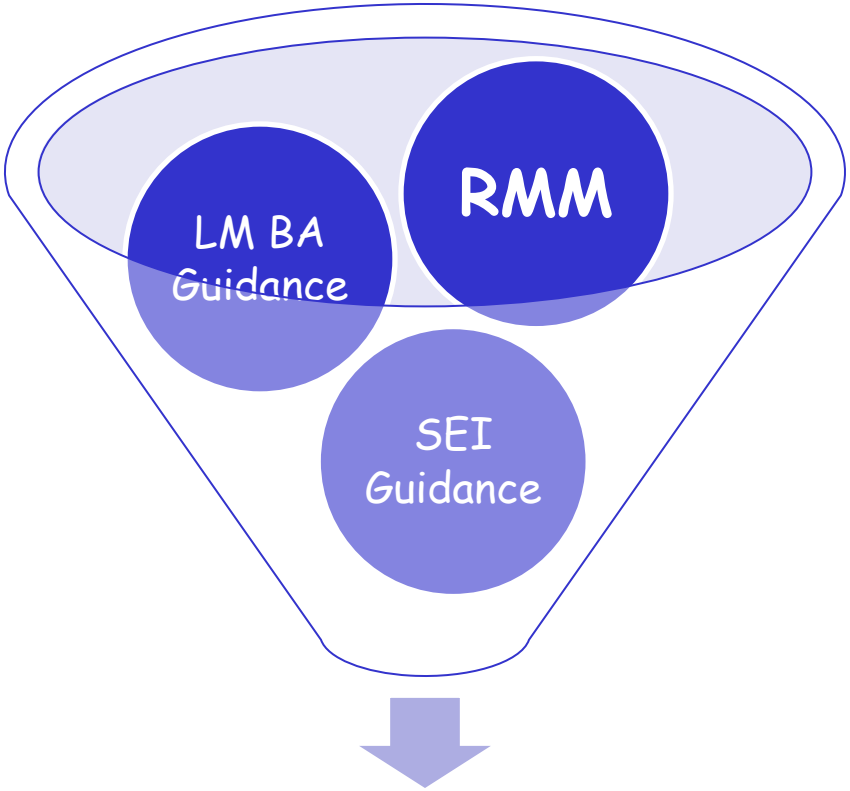
- Several Benefits
  - Early in development process
    - easily moldable for use within LM
  - Provides methods for appraisal similar to CMMI
    - Known among the SEI trained personnel at LM
  - Becoming an industry standard
    - Can use to measure ourselves against our peers and other industries
  - Contains a vast array of competencies in the DR/BC area

- *Still Requires Work*
  - Must filter process areas to use
  - Further define initial LM list of competencies to measure

Next Steps

- Further breakdown of defined competencies are required
  - Target DR/BC practices we want to develop within the company
  - Should be linked with RMM process area Specific Goals and Practices
    - Leverage RMM associated tools and artifacts
  - Work in collaboration with business area representatives to create
    - Initial work done in previous SIA events
- Must pick relevant RMM process areas
  - Funnel down to LM sought areas for improvement
  - Validate pared down RMM by SEI personnel
    - Work with David White and Lisa Young
- Create lower level competencies to help measure improvements which fill DR/BC gaps found within our own environment
- Pilot the focused RMM and funnel feedback to create final model

Approach



LM DR/BC Maturity Model