Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

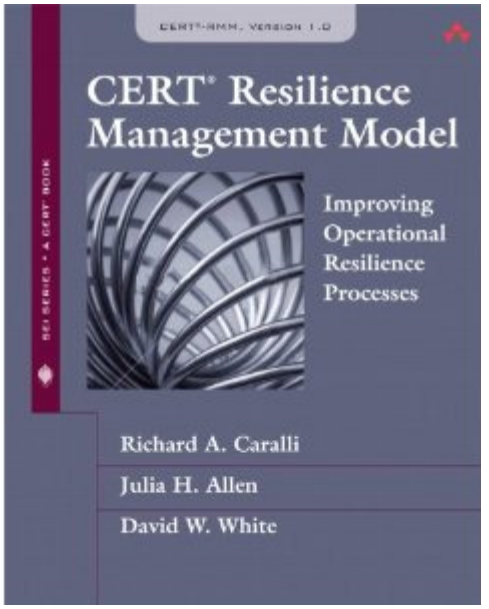
James F. Stevens

Software Engineering Institute

Adapting CERT-RMM to the Electricity Sector

Summary: Adapting CERT-RMM to the Electricity Sector

- **Outcomes:** A subset of CERT-RMM tailored to the electricity sector
- **Roadmap Challenge:**
  - Limited ability to measure and assess cyber security posture
  - No consistent cyber security metrics
  - Poor understanding of cyber risks
  - Weak business case for cyber security investments
- **Major Successes:** Presented RMM to leading utilities and received strong validation of need and applicability



- **Schedule:** pilot kickoff 9/10
- **Level of Effort:** $225K
- **Funds Remaining:** $215K
- **Performers:** SEI
- **Partners:** piloting utilities

Resilience defined

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

Parsed in organizational (and operational) terms:

> *The **emergent** property of an **organization** that can **continue to carry out its mission** after **disruption** that does not exceed its **operational** limit*

Where does the **disruption** come from? Realized risk.

CERT® Resilience Management Model

Capability maturity model—guidelines and practices for

- Converging of security, business continuity, and IT ops
- Achieving, managing, and sustaining operational resiliency
- Managing operational risk through process
- Measuring and maturing the resiliency process

Focuses on “what” not “how”

Organized into 26 process areas *(similar architecture to CMMI)*

Common vernacular and basis for planning, communicating, and evaluating improvements

Codifies best practices for security and business continuity from world leading organizations and numerous standards and codes

CERT-RMM at a glance

26 Process Areas in 4 categories

Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resiliency Requirements Development
RRM	Resiliency 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

Technical Approach and Feasibility

- **Approach**
  - CERT Resilience Management Model (CERT-RMM)
    - Process improvement model for implementing and managing security, business continuity, & IT operations
    - Based on years of CERT experience, research, and collaboration with high-performing organizations
    - Codified in 26 process areas, ~1000 pages of guidance
  - Identify and pilot a subset of CERT-RMM with electric power utilities
  - Evaluate applicability to and tailoring for sector

Technical Approach and Feasibility

- **Metrics for Success**
  - Pilot participants realize insight and value from the model
    - Model is useful for guiding implementation and ongoing operation of resilience activities
    - Comparison to model provides useful benchmarking, planning, and progress tracking
  - Model-based methods are lightweight enough to present low barrier of entry for utilities

Technical Approach and Feasibility

- **Challenges to Success**
  - Managing industry partner participation toward consensus/convergence on common approach
- **Technical Achievements to Date**
  - Industry buy-in on need for operational resilience management and improvement tools, and applicability of CERT-RMM

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - Project involves participation by industry experts to help select subset of model and by utilities to pilot the approach
    - Outreach activities in progress
    - Leading utilities have volunteered to participate
  - Next step to secure commitment to definitive project plan

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - Knowledge is intended to assist utilities in implementing and managing security, business continuity, and IT operations activities
  - Pilot success will be key in gaining industry support and adoption; objective is to generate success stories that can be used in outreach activities
  - CERT-RMM approach supports effective management of operational risk in a dynamic risk environment and calls for integration of activities that are often compartmentalized in organizations. Approach will leverage existing risk management activities.

Next Steps

- **Approach For the Next Year**
  - Perform pilot activities
  - Publish results report