James Stevens
Senior Member, Technical Staff - CERT® Division

James Stevens is a senior member of the technical staff in the CERT Program at Carnegie Mellon University’s Software Engineering Institute. James has been working in the information security field for over eighteen years and holds a BS degree in Electrical Engineering from the University of Notre Dame and an MBA from Carnegie Mellon University’s Tepper School of Business. James currently performs information and infrastructure security and resilience research and develops methods, tools, and techniques that support the secure and resilient delivery of critical services.
Notices

Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL 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 material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0000906
A Sampling of CERT-RMM Applications and Derivatives
Contents

1. ES-C2M2 History and Background
   • Challenge
   • Objectives
   • Approach
   • Results

2. Overview of ES-C2M2 Model
   • Domains
   • Scaling
   • Diagnostic Methodology
ES-C2M2 History and Background
Protecting the Nation’s Electric Grid from Cyber Threats

Protecting the electric system from cyber threats and ensuring its resilience are vital to our national security and economic well-being. This is exactly why cybersecurity is one of four key themes in the White House’s Policy Framework for a 21st Century Grid. For obvious reasons, the private sector shares our interest in a safe and secure electric grid. The Administration has benefited from working closely with industry, including to develop the Roadmap to Achieve Energy Delivery Systems Cybersecurity, released by the Department of Energy last September.

To continue that close cooperation, last week Deputy Secretary of Energy Dan Poneman and I, along with senior officials from Department of Homeland Security, hosted industry leaders to discuss a new initiative to further protect the electric grid from cyber risks. This initiative -- the Electric Grid Cybersecurity Risk Management Framework -- is a new White
ES-C2M2 Background

White House initiative

Led by Department of Energy

In partnership with Department of Homeland Security

In collaboration with representatives of electricity subsector asset owners and operators
ES-C2M2 Challenge and Objectives

Challenge:

Develop capabilities to manage dynamic threats and understand cybersecurity posture of the grid

Objectives:

• Strengthen cybersecurity capabilities
• Enable consistent evaluation and benchmarking of cybersecurity capabilities
• Share knowledge and best practices
• Enable prioritized actions and cybersecurity investments
ES-C2M2 Approach and Results

Approach:

• Create a maturity model and self-evaluation survey to develop and measure cybersecurity capabilities
• Encourage public–private collaboration effort
• Leverage existing guidance and knowledge

Results:

• A scalable, sector-specific model created in partnership with industry
ES-C2M2 Collaboration

And numerous utilities, including

Southern California Edison  Bonneville Power Administration  Pacific Gas & Electric
Electric Reliability Council of Texas  Dominion Resources  American Electric Power
Short Model-Development Time Frame

Jan. 5: Kickoff Meeting

Feb. 14: Advisory Group Working Session 2

Feb. 29: First draft model to Advisory Group

March 16: Revised draft model to Advisory Group and SMEs

March 29–May 4: Pilot Evaluations

Feb. 17: Draft domains to Advisory Group and SMEs for feedback

March 2: Advisory Group Working Session 3

March 22: Deliver pilot draft model and evaluation instrument for pilot

May 31: Initiative Closeout and Model Release

Jan. 2012

May 2012

Jan. 30: Advisory Group Working Session 1

Feb. 29: First draft model to Advisory Group

March 16: Revised draft model to Advisory Group and SMEs

May 29–May 4: Pilot Evaluations

May 14–15: Advisory Group Working Session 4
ES-C2M2 Resulting Artifacts

The Model


Self-Evaluation Tool Requests, Requests for Facilitation, & Questions

- ES-C2M2@doe.gov

- 94-page document
- The model itself is only 45 pages
ES-C2M2: Industry Use and Adoption

<table>
<thead>
<tr>
<th>Requesting entity type</th>
<th>Organizations¹</th>
<th>Individuals²</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Utilities</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cooperative (COOP)</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>International</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Investor-owned (IOU)</td>
<td>42</td>
<td>51</td>
</tr>
<tr>
<td>Public power (Muni)</td>
<td>37</td>
<td>47</td>
</tr>
<tr>
<td>Regional Transmission Organization (RTO)</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total Utilities</strong></td>
<td>99</td>
<td>118</td>
</tr>
<tr>
<td><strong>Non-utilities</strong></td>
<td>79</td>
<td>86</td>
</tr>
<tr>
<td>International</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>198</td>
<td>224</td>
</tr>
</tbody>
</table>

1. Total number of unique organizations that have received the ES-C2M2 Self-Evaluation Toolkit.
2. Total number of unique individuals who have received the ES-C2M2 Self-Evaluation Toolkit.
Using ES-C2M2

- Get Model & Tool
- Identify Gaps
- Prioritize and Plan
- Analyze Identified Gaps
- Perform Evaluation
- Implement Improvements
Overview of ES-C2M2 Model
A Maturity Model

Domains
(a.k.a. Process Areas)

Scaling

Diagnostic Methodology
Domains that ES-C2M2 Examines

- **RISK**
  - Risk Management

- **ASSET**
  - Asset, Change, and Configuration Management

- **ACCESS**
  - Identity and Access Management

- **THREAT**
  - Threat and Vulnerability Management

- **SITUATION**
  - Situational Awareness

- **SHARING**
  - Information Sharing and Communications

- **RESPONSE**
  - Event and Incident Response, Continuity of Operations

- **DEPENDENCIES**
  - Supply Chain and External Dependencies Management

- **WORKFORCE**
  - Workforce Management

- **CYBER**
  - Cybersecurity Program Management

Domains are logical groupings of cybersecurity practices.
ES-C2M2 Structure

10 Model Domains: Logical groupings of cybersecurity practices

1 Maturity Indicator Level that is reserved for future use

4 Maturity Indicator Levels: Defined progressions of practices

Each cell contains the defining practices for the domain at that maturity indicator level.
## Specific Characteristics for the ASSET Domain

<table>
<thead>
<tr>
<th>MIL0</th>
<th>1. Asset inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL1</td>
<td>a. There is an inventory of OT (operational technology) and IT (information technology) assets that are important to the delivery of the function.</td>
</tr>
<tr>
<td>MIL2</td>
<td>...</td>
</tr>
<tr>
<td>MIL3</td>
<td>a. The asset inventory is current and complete for assets of defined categories that are selected based on risk analysis.</td>
</tr>
<tr>
<td></td>
<td>b. Asset prioritization is informed by risk analysis.</td>
</tr>
</tbody>
</table>

Progress from one MIL to the next involves more complete or more advanced implementations of the core activities in the domain.

The organization is also expected to perform additional activities at higher levels consistent with its risk strategy.
## ES-C2M2 Maturity Indicator Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL0</td>
<td>Not Performed</td>
<td>• MIL1 has not been achieved in the domain.</td>
</tr>
<tr>
<td>MIL1</td>
<td>Initiated</td>
<td>• Initial practices are performed, but may be ad hoc.</td>
</tr>
<tr>
<td>MIL2</td>
<td>Performed</td>
<td>• Practices are documented.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stakeholders are involved.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Adequate resources are provided for the practices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Standards or guidelines are used to guide practice implementation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Practices are more complete or advanced than at MIL1.</td>
</tr>
<tr>
<td>MIL3</td>
<td>Managed</td>
<td>• Domain activities are guided by policy (or other directives).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Activities are periodically reviewed for conformance to policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Responsibility and authority for practices are clearly assigned to personnel with adequate skills and knowledge.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Practices are more complete or advanced than at MIL2.</td>
</tr>
</tbody>
</table>
A Dual-Progression Model

ES-C2M2 is a dual-progression model.

Two things progress across the maturity indicator levels:

1. Institutionalization – the extent to which the practices are ingrained in the organization’s operations

2. Approach – the activity’s completeness, thoroughness, or level of development/sophistication
Domain Structure

Domain

- Purpose Statement
- Introductory Notes
- Specific Objective(s)
  - Practices at MIL1
  - Practices at MIL2
  - Practices at MIL3
- Common Objective
  - Practices at MIL2
  - Practices at MIL3

Intent and overview

One or more progressions of practices that are unique to the domain

Progression of practices that describe institutionalization activities – same in each domain
Example Specific Objective: ASSET — approach progression

<table>
<thead>
<tr>
<th>Electricity Subsector Cybersecurity Capability Maturity Model Version 1.0</th>
<th>ASSET DOMAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3. Manage Changes to Assets</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **MIL1** | a. Changes to inventoried assets are evaluated before being implemented  
b. Changes to inventoried assets are logged |
| **MIL2** | c. Changes to assets are tested prior to being deployed, whenever possible  
d. Change management practices address the full lifecycle of assets (i.e., acquisition, deployment, operation, retirement) |
| **MIL3** | e. Changes to assets are tested for cybersecurity impact prior to being deployed  
f. Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality) |

Notice that the practices progress from one MIL to the next within the objective (practices at higher MILs are more complete in their implementation, more sophisticated in their approach, or more thorough).
Example Common Objective: ASSET — institutionalization progression

<table>
<thead>
<tr>
<th>4. Manage ASSET Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL1</td>
</tr>
<tr>
<td>MIL2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>MIL3</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### ES-C2M2: Maturity Indicator Levels

<table>
<thead>
<tr>
<th>Maturity Indicator Levels</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>X Reserved</td>
<td>Not applicable</td>
</tr>
<tr>
<td>3 Managed</td>
<td>Practices at levels 2 and 3 are progressively more complete, advanced, and ingrained</td>
</tr>
<tr>
<td>2 Performed</td>
<td>Level 1 practices are the starting point for any organization</td>
</tr>
<tr>
<td>1 Initiated</td>
<td>No practices at level 0</td>
</tr>
<tr>
<td>0 Not Performed</td>
<td></td>
</tr>
</tbody>
</table>
## Model Domains (1–2 of 10)

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
</table>
| Asset, Change, and Configuration Management (ASSET) | Manage the organization’s operational technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives, including activities to  
  - identify, inventory, and prioritize assets  
  - manage asset configurations  
  - manage changes to assets and to the asset inventory |
| Workforce Management (WORKFORCE)            | Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.  
  - Responsibilities  
  - Workforce controls  
  - Knowledge, skills, and abilities  
  - Awareness            |
## Model Domains (3–4 of 10)

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
</table>
| Identity and Access Management (ACCESS)    | Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.  
  • Identity management  
  • Access management |
| Risk Management (RISK)                      | Establish, operate, and maintain a cybersecurity risk management and mitigation program to identify and manage cybersecurity risk to the organization and its related interconnected infrastructure and stakeholders.  
  • Strategy  
  • Sponsorship  
  • Program |
# Model Domains (5–6 of 10)

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Supply Chain and External Dependencies Management (DEPENDENCIES)** | Establish and maintain controls to manage the cybersecurity risk associated with services and assets that are dependent on external entities, commensurate with the organization's business and security objectives.  
  - Dependency identification  
  - Risk management  
  - Cybersecurity requirements |
| **Threat and Vulnerability Management (THREAT)** | Establish and maintain plans, procedures, and technologies to identify, analyze, and manage cybersecurity threats and vulnerabilities, commensurate with the risk to critical infrastructure and organizational objectives.  
  - Threat management  
  - Vulnerability management  
  - Cybersecurity patch management  
  - Assessments |
## Model Domains (7–8 of 10)

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
</table>
| Event and Incident Response, Continuity of Operations (RESPONSE) | Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity incidents and to sustain critical functions throughout a cyber event, commensurate with the risk to critical infrastructure and organizational objectives.  
  • Detect events  
  • Declare incidents  
  • Respond to incidents  
  • Manage continuity |
| Situational Awareness (SITUATION) | Establish and maintain activities and technologies to collect, analyze, alarm, present, and use power system and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture, commensurate with the risk to critical infrastructure and organizational objectives.  
  • Logging  
  • Monitoring  
  • Awareness |
## Model Domains (9–10 of 10)

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Sharing and Communications (SHARING)</strong></td>
<td>Establish and maintain relationships with internal and external entities to share information, including threats and vulnerabilities, in order to reduce risks and increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.</td>
</tr>
<tr>
<td></td>
<td>• Communication</td>
</tr>
<tr>
<td></td>
<td>• Analysis</td>
</tr>
<tr>
<td></td>
<td>• Coordination</td>
</tr>
<tr>
<td><strong>Cybersecurity Program Management (CYBER)</strong></td>
<td>Establish and maintain a cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with the organization’s strategic objectives and the risk to critical infrastructure.</td>
</tr>
<tr>
<td></td>
<td>• Strategy</td>
</tr>
<tr>
<td></td>
<td>• Sponsorship</td>
</tr>
<tr>
<td></td>
<td>• Program</td>
</tr>
<tr>
<td></td>
<td>• Architecture</td>
</tr>
</tbody>
</table>
Using ES-C2M2

1. Get Model & Tool
2. Analyze Identified Gaps
3. Prioritize and Plan
4. Implement Improvements
5. Perform Evaluation

Flow: Get Model & Tool → Analyze Identified Gaps → Prioritize and Plan → Implement Improvements → Perform Evaluation → Get Model & Tool
ES-C2M2 Self-Evaluation

The ES-C2M2 model is supported by a survey-based self-evaluation.

An organization can use the survey (and associated scoring tool) to evaluate its implementation of the model practices.

To complete the survey, an organization selects its level of implementation for the model practice from a 4-point answer scale.
## 4-Point Answer Scale

<table>
<thead>
<tr>
<th>4-point answer scale</th>
<th>The organization’s performance of the practice described in the model is …</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully implemented</td>
<td>Complete</td>
</tr>
<tr>
<td>Largely implemented</td>
<td>Complete, but with a recognized opportunity for improvement</td>
</tr>
<tr>
<td>Partially implemented</td>
<td>Incomplete; there are multiple opportunities for improvement</td>
</tr>
<tr>
<td>Not implemented</td>
<td>Absent; the practice is not performed in the organization</td>
</tr>
</tbody>
</table>
There are 2 practices at MIL1 for the Risk Domain.

Outer ring and number(s) summarize implementation state of those practices; in this case, both practices are fully implemented.
Achieving MIL2 requires 13 practices in total, including the 2 from MIL1

11 practices are fully implemented

2 practices are not implemented
ES-C2M2 Sample Summary Score
ES-C2M2 Sample Summary Score
Introduction to the CERT Resilience Management Model

February 18 - 20, 2014 (SEI, Arlington, VA)
June 17 - 19, 2014 (SEI, Pittsburgh, PA)

See Materials Widget for course document