INSIGHT

Cybersecurity Capability Maturity Model (C2M2)

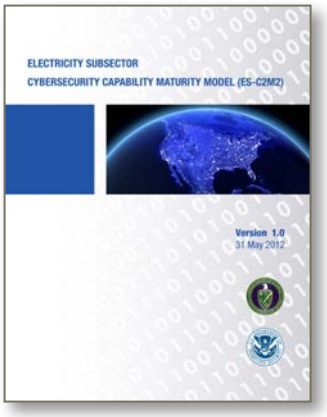
Author: Fowad Muneer, Senior Manager, ICF International

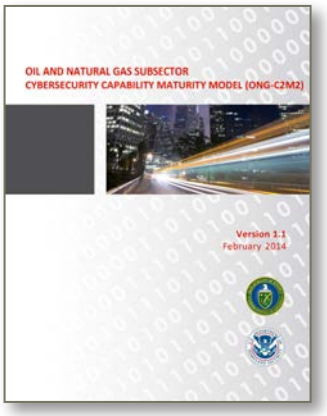
The cyber threat to critical infrastructure represents one of the most serious national and economic security challenges confronting the United States. The U.S. Government has numerous policies and programs to enhance the security and resilience of the nation's critical infrastructure. One example is the Cybersecurity Capability Maturity Model (C2M2) program under the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE).

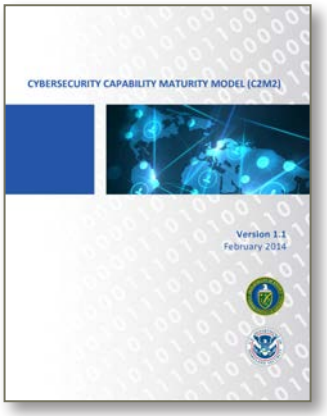
The C2M2 program comprises three maturity models:

- Electricity Subsector-Cybersecurity Capability Maturity Model (ES-C2M2)
- Oil and Natural Gas Subsector-Cybersecurity Capability Maturity Model (ONG-C2M2)
- Cybersecurity Capability Maturity Model (C2M2)

These models are a formalized process for evaluating the maturity of an organization's cybersecurity capabilities and are publicly available free of charge. The program, along with the models, also provides supporting toolkits, guidance resources, and self-evaluation facilitation support to the U.S. energy sector. The program's mission is strengthening the sector's security and resilience.







Background

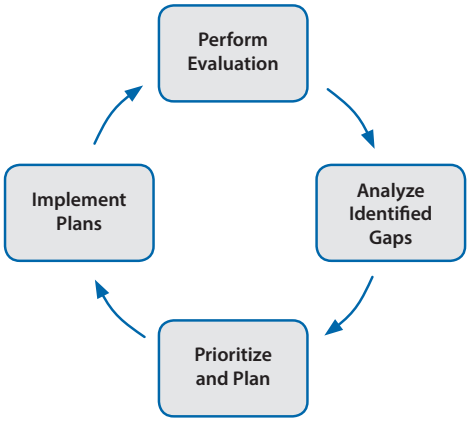
The C2M2 program was established in 2012 with the development of the archetype model ES-C2M2. The ES-C2M2 was the result of a White House initiative for the electricity subsector. The initiative was led by DOE, in partnership with the U.S. Department of Homeland Security (DHS) and in collaboration with public and private sector experts. In February 2014, DOE published Version 1.1 of ES-C2M2, ONG-C2M2 tailored for the oil and natural gas subsector, and a sector neutral C2M2.

Using the Model

The C2M2 can be used to:

- Effectively and consistently measure and benchmark cybersecurity capabilities.
- Prioritize actions and investments to improve cybersecurity.
- Share best practices across organizations as a means to improve cybersecurity capabilities.

An organization uses the model, supporting toolkit, reports, and resources to evaluate its capabilities, identify gaps, prioritize those gaps, and develop and implement plans. Over time, business objectives and the risk environment change, and the process is repeated.



Model Structure

The C2M2 is a scalable framework that can be used to measure capabilities on an enterprise-wide or functional basis. As a maturity model, it provides a set of characteristics that represent capability and progression in different cybersecurity areas. These characteristics are drawn from best practices, standards, and guidelines.

Domains

The model organizes cybersecurity practices into 10 groups called domains:

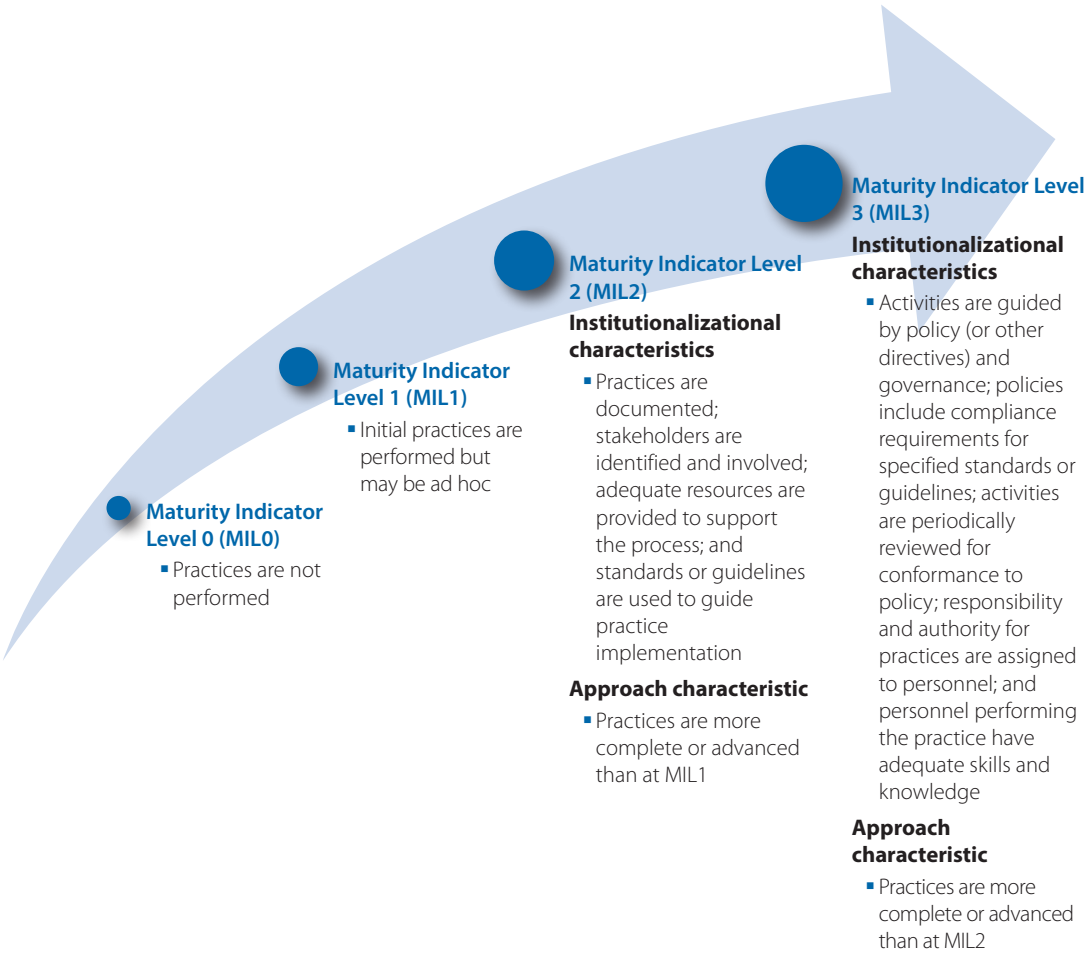
- Risk Management
- Asset, Change, and Configuration Management
- Identity and Access Management
- Threat and Vulnerability Management
- Situational Awareness
- Information Sharing and Communications
- Event and Incident Response, Continuity of Operations
- Supply Chain and External Dependencies Management
- Workforce Management
- Cybersecurity Program Management

The practices are further grouped within the domains under specific security and resiliency objectives for the domain. Practices listed under each objective within a domain are arranged in an order that represents increased maturity.

Maturity Indicator Levels (MIL)

The model defines four maturity indicator levels, MIL0 through MIL3. The MILs define a dual progression of maturity: an approach progression and an institutionalization progression. Approach progression refers to the completeness, thoroughness, or level of development of an activity in a domain. Institutionalization progression describes the extent to which a practice or activity is ingrained in an organization's operations. The more deeply ingrained an activity, the more likely the organization will continue to perform the practice over time, under times of stress, and in a consistent, repeatable manner. The figure below summarizes the characteristics of each C2M2 MIL. At MIL2 and MIL3.

The maturity indicator levels apply independently to each domain. For example, an organization could be operating at MIL3 in the Asset, Change, and Configuration Management (ACM) domain, MIL1 in the Supply Chain and External Dependencies Management (EDM) domain, and MIL0 in a third domain. Additionally, MILs are cumulative within each domain. In the above example to earn a MIL3 in the ACM domain, the organization must perform all of the practices in the MIL1, MIL2, and MIL3 levels. The C2M2 does not suggest achievement of the highest MILs as an automatic goal. Instead, target MILs for different domains should be based on the organization's business objectives, cybersecurity strategy, and its costs and benefits analysis.



Source: http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program

icfi.com

About ICF International

ICF International (NASDAQ:ICFI) provides professional services and technology solutions that deliver beneficial impact in areas critical to the world's future. ICF is fluent in the language of change, whether driven by markets, technology, or policy. Since 1969, we have combined a passion for our work with deep industry expertise to tackle our clients' most important challenges. We partner with clients around the globe—advising, executing, innovating—to help them define and achieve success. Our more than 5,000 employees serve government and commercial clients from more than 70 offices worldwide. ICF's website is www.icfi.com.

Conclusion

The C2M2 is an easy, flexible, and cost-effective tool for improving an organization's cybersecurity capabilities. Organizations typically hold a day-long collaborative session for their security and resilience stakeholders. Practices are determined to be fully implemented, largely implemented, partially implemented, not implemented, or not applicable; and the answers are recorded in the C2M2 toolkit. The toolkit processes the answers and generates summary and detailed reports that include dashboard representation of strengths and gaps.

ICF International's cybersecurity experts participated in the development of the ES-C2M2 and its derivative models. ICF supports DOE in C2M2 program management activities. For further information, contact David McGill at +1.703.934.3725 or Greg Frank at +1.444.573.0540.

icfi.com/cyber