C2M2 The Energy Sector's Step-by-Step Process for Implementing the NIST Cyber Security Framework (CSF)

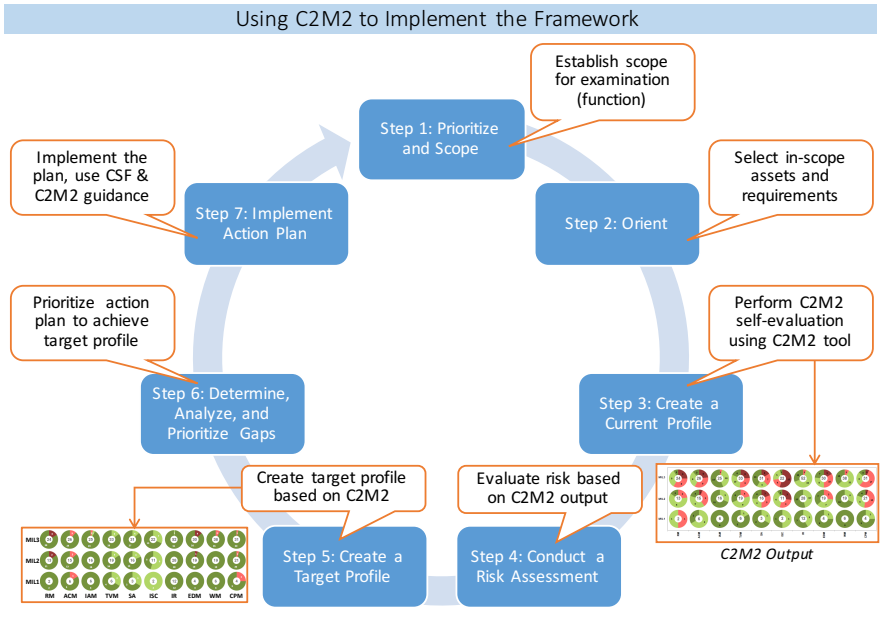
Energy sector business and security leaders are committed to ensuring appropriate cybersecurity of their operations. Many energy firms are using the Cybersecurity Capability Maturity Model (C2M2) to evaluate their cyber maturity and plan improvements. Sector leaders are also interested in adopting the NIST Cyber Security Framework as part of the cyber program.

The good news is that using the C2M2 is a solid approach for implementing the Framework that has specific benefits for energy sector firms. **Organizations that are using the C2M2 to inform their cyber program evolution can confidently claim that they are implementing the Framework.**

Top benefits of using C2M2 to implement the Framework:

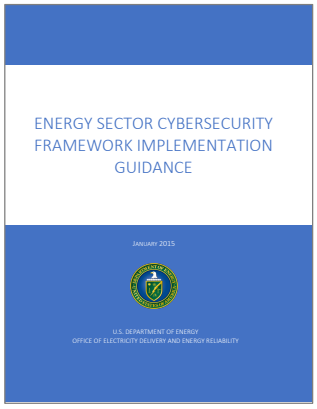
- ***Enables benchmarking***: C2M2 includes a defined, tool-based evaluation method that produces results that can be used for benchmarking within organizations and across the sector.
- ***Energy-specific guidance***: C2M2 has two variants that have been tailored to address specific concerns of the Oil and Natural Gas (ONG-C2M2) and Electricity (ES-C2M2) subsectors.
- ***Complete Framework coverage***: A Department of Energy (DOE) mapping shows that the C2M2 addresses ***all*** Framework components (Subcategories and Tiers).
- Additional benefits are outlined in the ***Energy Sector Cybersecurity Framework Implementation Guidance***, official DOE advice to energy firms for implementing the Framework.

The Framework defines a specific process for implementation. The diagram below shows how the C2M2 is optimally used to accomplish that process.



About the C2M2:
C2M2 was developed by and for energy sector firms under the leadership of the DOE. C2M2 includes an easy-to-use self-evaluation toolkit that produces a graphical summary of results and is available in three versions: Oil and Natural Gas (ONG-C2M2), Electricity (ES-C2M2), and generic (C2M2). The three model versions contain exactly the same 312 practices, organized into the same 10 domains, so the results from any of the model versions are completely comparable.

About the Framework:
The National Institute of Standards and Technology (NIST) developed the Framework for Improving Critical Infrastructure Cybersecurity in response to Executive Order (EO) 13636 "Improving Critical Infrastructure Cybersecurity." The Framework recommends risk management processes that inform and prioritize decisions regarding cybersecurity based on business needs, without imposing regulatory requirements.



DOE Guidance:
Detailed guidelines for Framework implementation by energy firms is available on the DOE website[1]. The guidance includes a detailed mapping of Framework elements to C2M2 practices.

[1] http://energy.gov/oe/downloads/energy-sector-cybersecurity-framework-implementation-guidance