

Cyber Security Update and Future Direction

Matthew Light
ES-C2M2/RMP Program Manager
U.S. Department of Energy



Electricity Subsector Cybersecurity Landscape

- Emerging technologies, convergence of Information Technology (IT) and Operational Technology (OT)
- Increased connectivity across traditionally segmented operations has increased the cyber risks to the missions and business processes of electricity subsector organizations.
- Large number of diverse federal, state, regulatory and private stakeholders across the subsector have differing cybersecurity expectations and objectives.
- Their understanding of industry operations and cybersecurity varies and is framed by their own organization's mission.

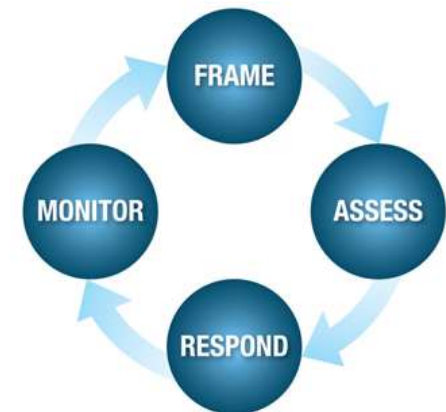
Risk Management Process (RMP) Guideline

- Developed by Department of Energy (DOE) in collaboration with National Institute of Standards and Technology (NIST), North American Electric Reliability Corporation (NERC), and subject matter experts from across the electricity subsector.
- Provide a consistent, repeatable, and adaptable process for risk management across the entire electricity sector
- Help utilities better manage cybersecurity risks using a mission & business process focused approach.
- Can be applied to any electricity subsector organization regardless of size or type.



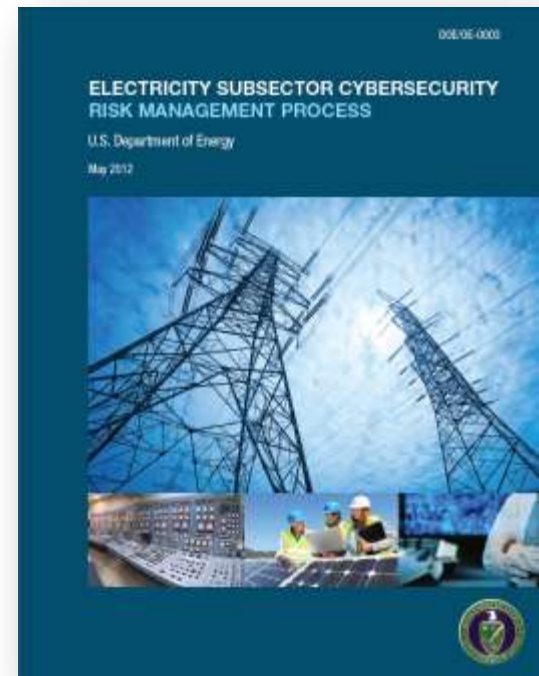
Risk Management Process (RMP) Guideline

- To facilitate a comprehensive view of how risk management activities are undertaken across the organization, the guideline presents organizations as a three-tiered structure referred to as the 'Risk management model'.
- The process referred to as the 'Risk management cycle' is constantly re-informed by the changing risk landscape as well as changing organizational priorities and functions.
- The RMP is based on integrating the risk management cycle at each business tier in the risk management model.



Risk Management Process (RMP) Guideline

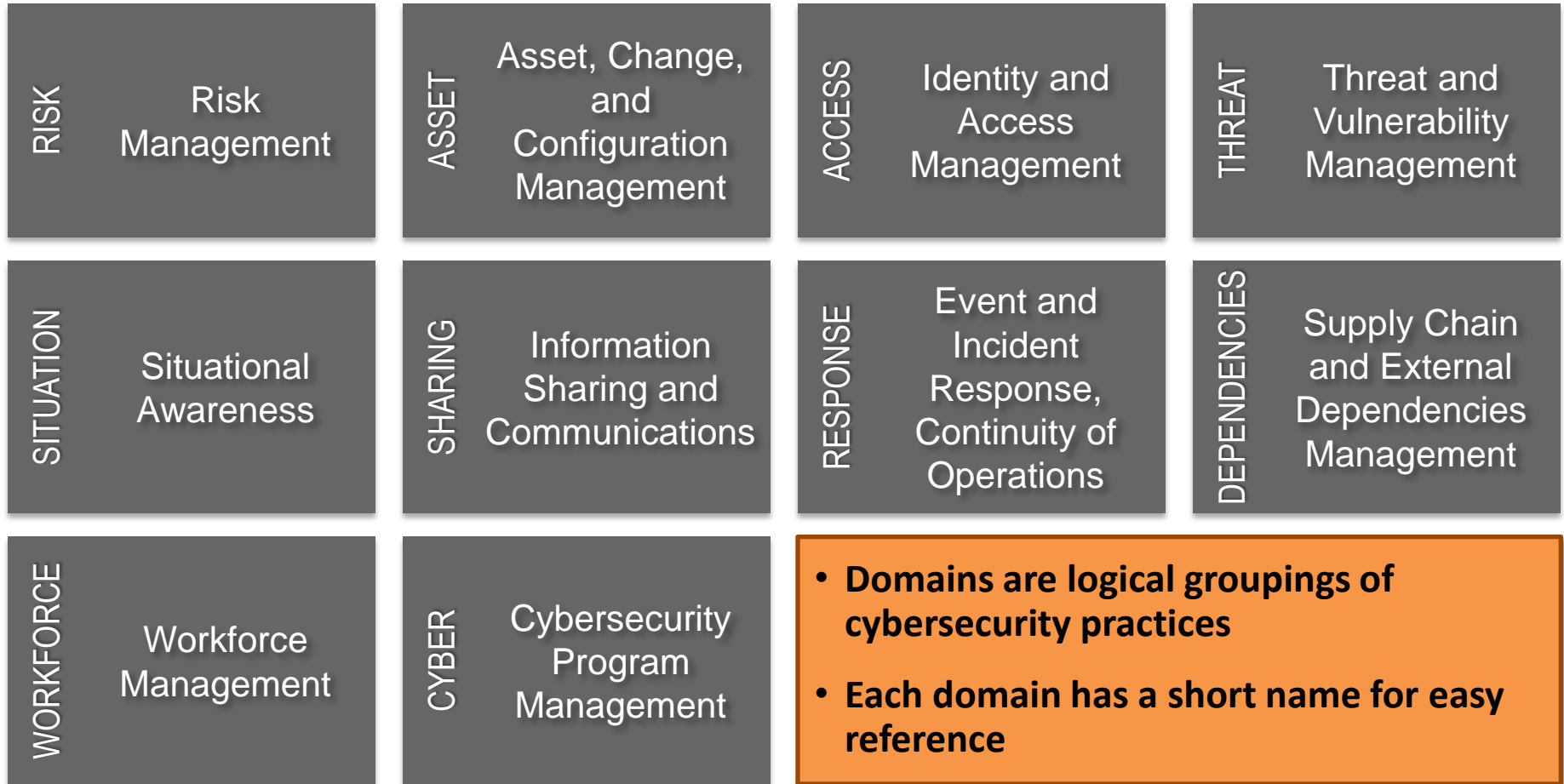
- The RMP guideline is available for downloading at:
<http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012>.
- DOE will partner with private sector organizations interested in voluntary pilot implementation of the RMP
- RMP Program information can be obtained by emailing RMPGuideline@HQ.DOE.GOV



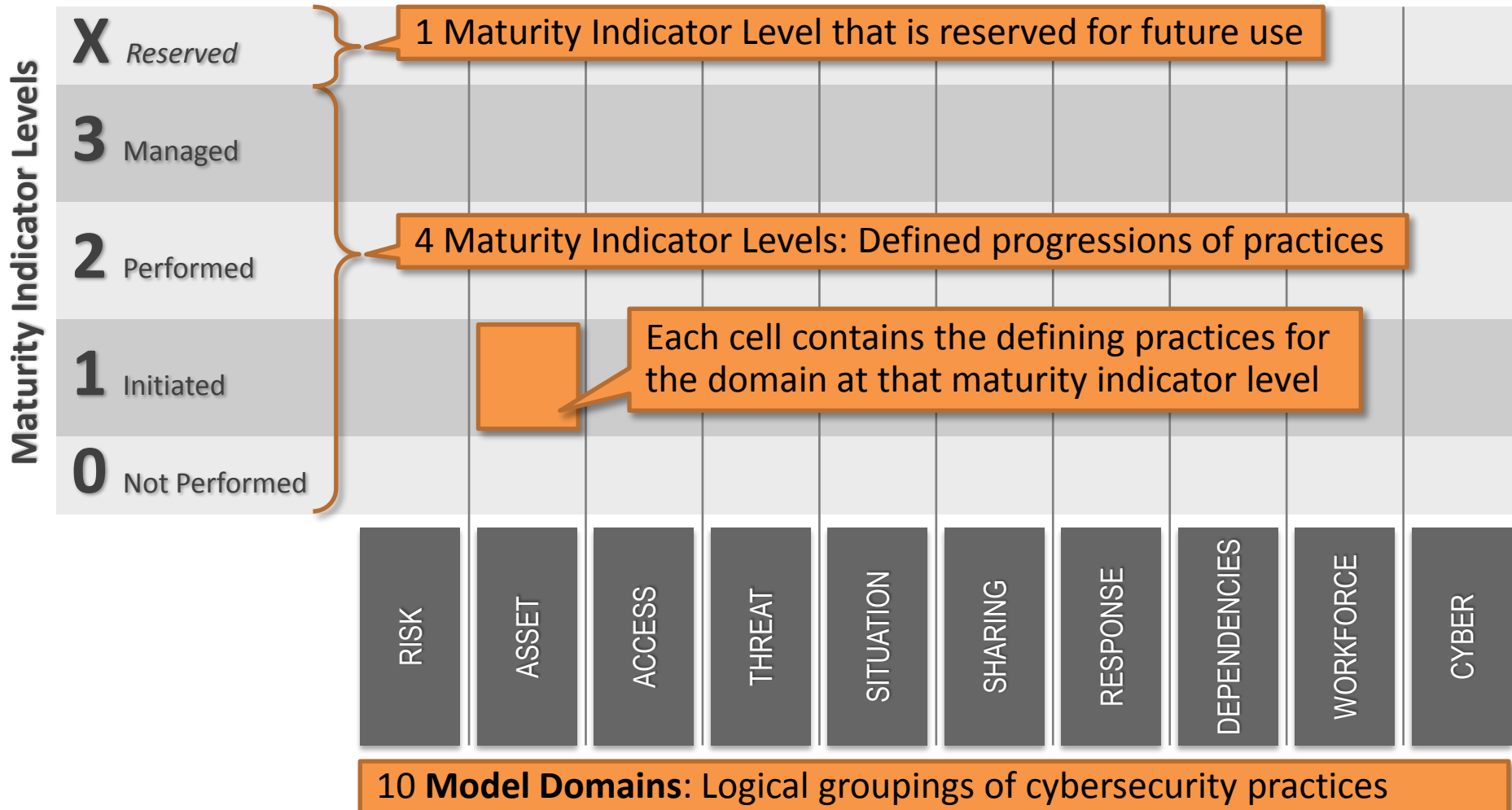
Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

- Objectives:
 - Strengthen cybersecurity capabilities
 - Enable consistent evaluation and benchmarking of cybersecurity capabilities
 - Share knowledge and best practices
 - Enable prioritized actions and cybersecurity investments

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)



Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)



Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

- The ES-C2M2 is available for download at: <http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012>
- ES-C2M2 program information can be obtained by emailing ES-C2M2@HQ.DOE.GOV

