Operational Technology
Cybersecurity Coalition

Sector Risk Management Agency Maturity Model

Abstract

Recent cyberattacks on critical infrastructure have underscored a persistent challenge: the inconsistent cybersecurity maturity across the federal government's Sector Risk Management Agencies (SRMAs). To address this critical national security gap, this document proposes a new framework for the Office of the National Cyber Director (ONCD) to evaluate and improve the cybersecurity capabilities of these agencies. The model would enable ONCD to annually evaluate SRMAs on a 1-to-5 scale based on their domain expertise, policies, risk assessments, incident response, and cross-sector coordination—especially in operational technology (OT) environments. The framework is designed to align with existing mandates and standards, while establishing consistent benchmarks for federal budgeting, sector-specific performance metrics, and collaboration with industry. The overarching goal is to enhance national critical infrastructure resilience by identifying SRMA gaps, guiding investment, and enabling both public and private sectors to plan for continuous cybersecurity improvement.

About the OTCC

The Operational Technology Cybersecurity Coalition is a diverse group of leading cybersecurity vendors representing the entire OT lifecycle. The OT Cyber Coalition believes that the strongest, most effective approach to securing our nation’s critical infrastructure is one that is open, vendor-neutral, and allows for diverse solutions and information sharing without compromising cybersecurity defenses.

Authors

Tatyana Bolton
Executive Director
Operational Technology Cybersecurity Coalition (OTCC)

Mark Montgomery
Center on Cyber and Technology Innovation Senior Director and Senior Fellow
Foundation for Defense of Democracies (FDD)

Sector Risk Management Agency Categories of Maturity

1 Inconsistent Maturity

- Possesses limited cybersecurity domain expertise. Security policies are outdated (older than 5 years old). Does not pursue any risk assessment. Does not have incident response plans. Does not have any cross-sector coordination or information sharing.

2 Basic Maturity

- Presence of initial domain expertise within the SRMA; the SRMA is working to understand what cybersecurity needs are both important and unique to the sector.
- Working to develop basic security policies (Risk Management, Access Controls, Vulnerability Management, Incident Response Plan). Policies may lack regular updates.
- Working to establish basic sector risk assessment processes.
- Basic incident response plans but may lack testing, coordination, or clear responsibilities. Published sector incident response plan, but lacks sufficient training and annual reinforcement.
- Nascent information sharing efforts without consistent and coordinated processes.

3 Structured Maturity (All Items for 2 Above, Plus)

- The SRMA has an overview of the entities within the sector. Well-documented and updated guidance, such as risk management, aligned with industry best practices.
- Regular sector risk assessments are performed, and risk management strategies are updated for critical entities and systems.
- Annual tabletop exercise with CISA and the FBI to test the agency response plan; sector partners to test the sector response plan. Annual cross sector tabletop exercise with sector partners as well as agencies/sectors that represent significant interdependencies.
- Detailees from agency to CISA watch floor, and from CISA to agency, to build relationships and understanding of roles/responsibilities of agency and CISA. SRMA conducts regular marketing efforts to drive adoption of CISA's free cyber hygiene tools.

4 Managed Maturity (All Items for 2 and 3 Above, Plus)

- Security policies and procedures are regularly reviewed, updated, and effectively communicated across the sector. The SRMA has Cyber Performance Goals for its sector and manages those with sector partners.
- Regular sector risk assessments are performed, and risk management strategies are updated for all entities and systems. The SRMA must conduct an annual "census" of their industry to assure that the SRMA engages the sector at a statistically significant level.
- Well-established incident response capabilities, continuous monitoring, and regular drills or simulations.
- Clear and delineated roles and responsibilities between SRMAs, ISACs, and Sector Coordinating Councils (SCCs). 70 percent of the sector participates in industry's ISAC and SCC.

5 Optimized Maturity (All Items for 2, 3 and 4 Above, Plus)

- For each National Critical Function, the SRMA must work with CISA, the sector, and their Sector Coordinating Councils to identify minimum viable delivery objectives for services.
- The SRMA must produce an annual report to the DHS CISA National Risk Management Center and the ONCD.
- SRMA can map and measure interdependencies that its sector has with other critical infrastructure sectors. Shows consistent improvement and strives to advance security across ecosystem partners and other sectors.