Cybergovernance Maturity Oversight Model (CMOM)

CYBERNANCE
First In Cybergovernance

Cyber Risk Oversight for Financial Services Firms

Objectives

1) Meet regulatory scrutiny head-on.
Use NIST to align with SEC guidance and FFIEC exams.

2) Ease board concerns about cyber risk.
Protect the organization by benchmarking against standards.

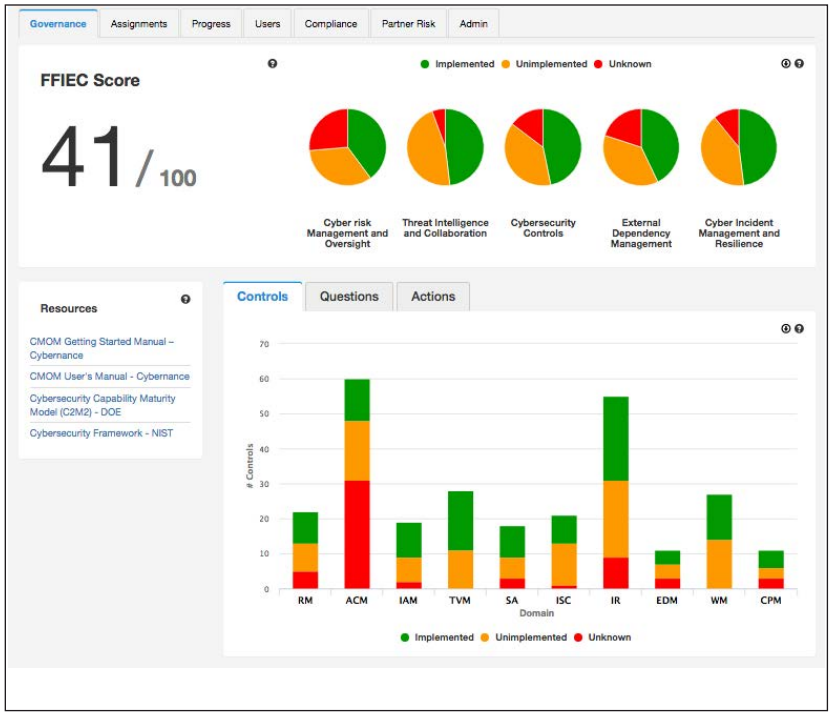
3) Rank and rate vendors on their cyber capability.
Gain visibility into partners' ability to align with NIST.

Observations

- FINRA launched "sweeps" examinations in 2014 to target cybersecurity at broker-dealers.
- Guidance centers on using the NIST Cybersecurity Framework.
- Boards of directors should play a leadership role in overseeing firms' cybersecurity efforts.

The Value of CMOM

- Operate confidently under the eye of FFIEC and other regulators.
- Exercise diligence and control over supply chain cyber risk.



Guidance issued in FINRA's 2015 Report on Cybersecurity Practices suggested that financial services firms adopt accepted standards from NIST to address cyber risk. The CMOM Platform does exactly that. Our software uses the NIST Cybersecurity Framework to evaluate and report your firm's cyber resilience in terms put forth by the FFIEC. We monitor 300 control points across the organization, going beyond technology to examine people, process, and policies that impact cyber risk.

CMOM's reporting functions give you the capability to demonstrate your alignment with FFIEC principles, which were built using the contents of the NIST Cybersecurity Framework. By benchmarking the organization against this standard, your firm can identify gaps and take action to improve cyber resilience over time.

Contact us with specific questions, or to set up a live demo: info@cybernance.com.

Pressure to manage cyber risk is everywhere. Use the NIST standards to your advantage.