ISACA®

CMMI® Institute
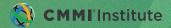
CYBERSECURITY MATURITY ASSESSMENT

To optimize your cybersecurity program—people, processes, technology—ISACA and CMMI recommend an enterprise-wide capabilities and risk assessment, starting with revamped workflow.

THE ENTERPRISE ASSESSMENT WORKFLOW

Board

CISO

Operations Level

CISO

Define the scope of the assessment and the organization's risk profile; risk-based maturity targets are defined

RISK PROFILE

RISK-BASED MATURITY TARGETS

- Evaluate/assess risk profile
- Assess threats (internal/external)
- Set risk targets per risk appetite
- Set/review/validate KPIs
- Set total cost of ownership targets for risk control measures

---

Select practices to determine practice area maturity level; determine industry standards and compliance levels

ISO/CSF/COBIT THREAT VIEW

MEASURED MATURITY VS. RISK-BASED TARGETS

MEASURED MATURITY VS. INDUSTRY BENCHMARKS

RISK-PRIORITIZED GAPS AND SOLUTIONS

- Set controls, risk-mitigation measures
- Measure control resiliency
- Collect cost of ownership data
- Validate tie between controls and risks
- Measure against KPIs and report performance

Develop risk-mitigation roadmap

MEASURED MATURITY VS. INDUSTRY BENCHMARKS

PRIORITZED CYBERMATURITY ROADMAP; INVESTMENT PRIORITIES

- Validate maturity/resilience targets
- Review/assess cost of ownership data against risk targets
- Prioritize remediation and gaps
- Summarize/consolidate metrics

Define organizational priorities; approve cybersecurity roadmap and investment priorities

- Validate organizational risk appetite
- Review and approve priorities
- Consume summarized metrics