ISACA
CMMI Performance Solutions

CMMI® SECURITY Battlecard

Value Proposition

Improves performance and key capabilities for organizations to assess, enhance, and improve their approach to security beyond compliance.

Target Audience

Organizations that want to improve their approach to security beyond compliance.

Audience Pain Points:

- Spending too much time reacting to threats
- Low customer confidence

Key Benefits

- Increase customer confidence.
- Enhance resiliency
- Improve employee morale and turnover
- Easily integrate popular standards and requirements

Relation to Government Mandates, Standards and Methodologies

- FedRAMP
- S-BOM
- CMMC
- NIST CSF 2.0, 800-171, 800-171A
- ISO 27000, 27001
- EDA Cyber Code of Practice

Proof Points

- Significant decrease in network attacks in July and August: 49% in July and 79% in August
- Reduced time to identify threats: the previous average was greater than 72 hours, the current average is less than 12 hours
- Reduced time to resolve security threats: the previous average was approximately 4 hours; the current average is 15 minutes
- **Phoenix Defense Case Study**

> "The new CMMI Security and Managing Threats practice areas gave us the perfect framework to complete and complement our NIST 800-171 and CMMC security practices while we wait on the official CMMC ver. 2.0 guidelines."
>
> — **Richard Stikkers,** Chief OperatingOfficer Phoenix Defense

Practice Areas

- **Enabling Security:** Reduces the impact of security threats and vulnerabilities on business performance.
- **Managing Security Threats and Vulnerabilities**: Increases an organization's capability and resilience to identify, mitigate, and recover from threats and vulnerabilities.

Differentiators

- With its open architecture, CMMI not only works well and easily integrates with other standards and frameworks, it enables them to be more useful and effective for building capability and improving performance
- The CMMI has been and continues to be applicable to a broad range of organizations, domains, technologies, or contexts.

Why Adopt Multiple Domains?

- Multiple domains in a single appraisal event will yield cost and resource savings.
- Provides the opportunity to look beyond a single domain to where there is overlap in the Organizational Unit's (OUs) processes to add continuous improvement value and identify the opportunity for further process integration.
- Enables appraisal teams to more easily understand and see how processes are performed in the OUs, projects, and organizational support functions (OSFs).
- Model scope with multiple domains reflect how work is performed across industries, geographies and OUs.