SHIELDManagement
Product Suite

IT CONSULTING AND SOLUTIONS

INTENT

CTI's SHIELDManagement suite is intended to provide organizations with assistance in the administration and operational management of their information security program. SHIELDManagement engagements provide organizations with highly-qualified security professionals to assist with the design, implementation, and maintenance of the organization's information security program. The ultimate goal of CTI's SHIELDManagement suite is to enhance and strengthen the confidentiality, integrity, and availability of the organization's IT systems and information assets. Flexibility in scope allow for multiple functions to be included in SHIELDManagement engagements, allowing management efforts to be tailored to meet your organization's budget and needs. CTI can provide resources as needed or on a scheduled basis.

COMPONENTS

The following graphic illustrates the various functions available as part of CTI's SHIELDManagement product. These services can be scheduled and tailored to fit your needs.

SHIELDManagement Administration	**SHIELDManagement** Operations
• Board and Steering Committee Presentations	• Change Control Review
• Information Security Program Development or Maintenance	• Configuration & Hardening Review
• Plan of Actions and Milestones Development	• Data Loss Prevention
• Policy, Standard, and Procedure Development	• Incident Response
• Risk Management	• Patch Management
• Security Awareness Training & Education	• Security Event Review
• Security Compliance Management	• Security Architectural Review
	• Social Engineering Exercises
	• Vulnerability Management

SECURITY HEALTHCHECKS | INTERNAL EVALUATIONS | LOGISTICAL DOCUMENTATION

DETAIL OF FUNCTIONS

- **Board of Directors and Steering Committee Presentations** – CTI can provide a resource to update senior management, Board of Directors, or other steering committees on the organization's information security program.

- **Information Security Program Planning** – Assist the organization with strategic planning for the organization's information security program and maintain established plans to reflect a changing cybersecurity landscape.

- **Plans of Actions and Milestones (PoAM)** – Develop a PoAM based on assessment results from internal or external stakeholders to ensure specific goals are achieved as it related to the information security program.

- **Policy, Standards, and Procedures** – Create and develop policies, standards, and procedures that support the information security program and allow the organization to achieve its vision.

- **Risk Management** – Perform periodic risk assessments of the organization and participate in discussions related to the risk treatment.

- **Security Awareness Training** – Provide education on a periodic basis to the organization's workforce or specific departments to facilitate awareness of information security risks across the organization.

- **Vendor Management** – Assist with the development of a vendor management program and establish vendor risk assessment and business associate due diligence practices.

- **Change Control Review** – Evaluate the risk related to changes made to the IT environment to minimize impact on the organization's security posture and solidify the IT change process.

- **Configuration & Hardening** – Review current infrastructure to ensure systems have been hardened in accordance with industry-standard guidelines such as CIS, NIST, or SANS.

- **Data Loss Prevention** – Evaluate sensitive data that could be exfiltrated from the organization, report it to management, and guide modifications to controls to help prevent further data loss.

- **Incident Response** – Assist with response to security incidents through activation of the organization's security Incident Response plan.

- **Security Event Review** – Periodically review system and application security logs to detect and address any anomalous behavior on the network.

- **Social Engineering Exercises** – Perform phishing simulations to evaluate organizational awareness of common phishing attack methods and provide follow-up training when necessary.

- **Vulnerability Management** – Perform internal and external vulnerability scans of the IT environment to identify areas where remediation may be necessary.

SECURITY HEALTHCHECKS | INTERNAL EVALUATIONS | LOGISTICAL DOCUMENTATION