

SHIELDControls Product Suite



INTENT

CTI's SHIELDControls suite is intended to evaluate the devices, systems, policies, procedures, and practices in place to protect the customer's information security environment and all assets contained therein. The three assessments comprising the SHIELDControls suite provide varying degrees of review and documentation suitable for diverse needs and budgets. Recommendations for new controls and configuration guidance for existing controls are provided to help eliminate any identified vulnerabilities. As a result, organizations are able to understand how thoroughly their corporate security controls are configured, which – if any – recommended controls are missing, and what steps need to be taken to improve the customer's information security posture. NOTE: the Core and Pro offerings can be customized to certain compliance standards for customers with regulatory requirements.

COMPONENTS

The following graphic illustrates the various assessments available as part of CTI's SHIELDControls suite. These services range from concise one- to three-day engagements to detailed multi-week assessments.

SHIELDControls Pro

SHIELDControls Pro is CTI's most comprehensive security controls assessment. Drawn from the ubiquitous NIST SP 800-53 standard, this assessment dives into the configuration of over 25 of the customer's administrative, technical, and physical controls. Control configurations are rated using a detailed scoring system that grants the organization a thorough understanding of their security environment.

Assessment highlights: customized, actionable recommendations, a review of the organization's physical security controls, a network perimeter vulnerability assessment, as well as a granular review of security policies and other administrative controls.

SHIELDControls Core

SHIELDControls Core is CTI's most popular security assessment, evaluating the customer environment from the perspective of CIS's Top 20 Critical Security Controls list. The resulting documentation provides the customer a qualitative understanding of their security posture, as well as customized, actionable risk findings and remediation recommendations. This assessment includes a physical security evaluation as well as a security policy spot check.

SHIELDControls Express

Looking to evaluate your organization's security posture for the first time but don't know where to start? CTI's SHIELDControls Express leverages the NIST SP 800-171 standard to efficiently and effectively evaluate the presence of controls from up to seven (7) security categories. This quick and painless analysis is the perfect way to identify high-level discrepancies in security practice, allowing for accurate security budgeting and goal-setting.

SECURITY HEALTHCHECKS | INTERNAL EVALUATIONS | LOGISTICAL DOCUMENTATION

BREAKDOWN

The following table examines the differences between the levels within the SHIELDControls Product Suite.

	SHIELDControls Express	SHIELDControls Core	SHIELDControls Pro
Appropriate for review by regulatory auditors?	Not recommended	Yes	Yes
Level of customer participation required	Minimal	Moderate	Significant
External assessment included?	No	Optional	Yes
Physical controls evaluation included?	No	Yes	Yes
Policy review included?	No	Policy type checklist	In-depth review
Level of automated scanning?	None	System patch distribution validation	Patch validation and vulnerability scanning
Applicable regulatory standards?	N/A	HIPAA, GLBA, FFIEC, HITRUST, SOX, etc.	HIPAA, GLBA, FFIEC, HITRUST, SOX, etc.
Recommendation style?	Universal best practices	Customized, actionable	Customized, actionable
Control evaluation method?	7 NIST control families	CIS Top 20 Critical Controls	14 NIST control families + CIS Top 20 Critical Controls
Control scoring method?	Percentage of deployed vs. not deployed	Qualitative rating	Quantitative rating
Average assessment duration?	2-3 days	5-7 days	7-10 days
Approx. # of controls evaluated?	7	20	25+
Foundational standard	NIST SP 800-171	CIS Top 20 Critical Controls	NIST SP 800-53
Delivery meeting included?	Yes	Yes	Yes

ADDITIONAL OPTIONS

Additional testing and assessments can be added to certain levels within the SHIELDControls Suite:

- Evaluate all 14 NIST control families instead of only 7. (Express only)
- Include network perimeter vulnerability assessment. (Core only)
- Include internal / external penetration testing. (Core & Pro only)
- Include phishing / social engineering testing. (Core & Pro only)
- Include a Business Impact Analysis (BIA). (Core only)

SELECTION

Answers to the following questions will help determine which level of service your organization should select:

- 1) Approximately how many servers do you have in your environment? (Virtual and/or Physical)
- 2) About how many business units (departments) are in your organization?
- 3) Is your organization subject to any regulatory requirements?
- 4) How many physical office locations would be visited during this assessment?

