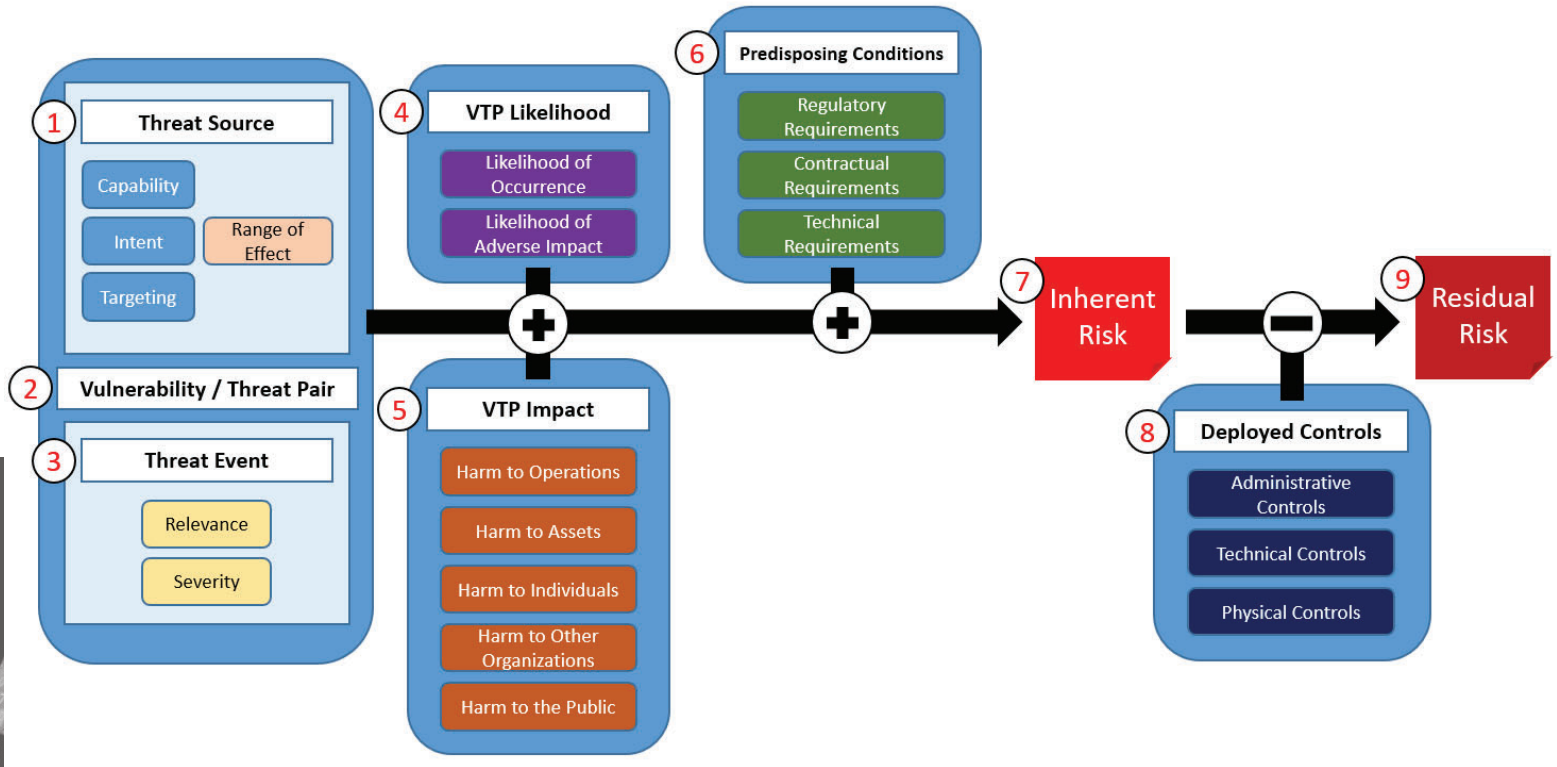
SHIELDRisk
Product Suite

CTI
IT CONSULTING AND SOLUTIONS

INTENT

CTI's SHIELDRisk product suite provides organizations with a comprehensive understanding and analysis of the current threats to its assets, both digital and physical. SHIELDRisk assessments systematically determine how identified risks impact the organization's environment, what security controls are implemented (if any) to mitigate those risks, and how effectively those controls are deployed and configured. Increasing organizational awareness and understanding of information security risks also helps prioritize remediation efforts. These assessments also provide the foundation for a security roadmap to be created and communicated to executive stakeholders, driving support for the organization's Information Security program. SHIELDRisk assessments can also be tailored to evaluate your compliance with regulatory standards (e.g. DFARS, FFIEC, HIPAA, HITRUST, NIST, and PCI).

PROCESS MAP



SECURITY HEALTHCHECKS | INTERNAL EVALUATIONS | LOGISTICAL DOCUMENTATION

CTI | 235 Schilling Circle, Suite 100, Hunt Valley, MD 21031 | www.webcti.com | 800-606-6060 | info@webcti.com

PROCESS SUMMARY

1. Create Vulnerability / Threat Pairs – Vulnerability / Threat Pairs (VTPs) are scenarios that describe a particular risk to the organization. CTI consultants consider a variety of factors during the creation of VTPs, including the organization's industry, location, workforce profile, and workplace environment. Threat sources and threat events are combined to create a focused VTP. Steps 1 through 3 of the Process Map above describe the VTP creation process.

2. VTP Likelihood – Once a Vulnerability / Threat Pair (VTP) has been established, CTI consultants evaluate the likelihood that the specific vulnerability or risk will occur and have an adverse impact on the organization. Step 4 on the Process Map above describe the VTP Likelihood estimation process.

3. VTP Impact – Having established the likelihood that a VTP will occur, CTI consultants seek to understand the full spectrum and degree of impact the risk will have on an organization, its assets, workforce, partners, and the public in general. Step 5 on the Process Map above describe the VTP Impact estimation process.

4. Inherent Risk Calculation – With the estimated Likelihood and Impact of a given VTP documented, CTI will use these factors to calculate the Inherent Risk for that scenario. Any predisposing conditions (e.g. regulatory or contractual requirements) that may further increase an element of the risk to the organization are considered here as well. Steps 6 and 7 on the Process Map above describe the Inherent Risk calculation process.

5. Residual Risk Calculation – Finally, CTI consultants will review the controls currently deployed by the organization and estimate their effectiveness in reducing the impact and likelihood levels of the risk described in the VTP. From this, a residual risk level is discerned and presented to the customer for review and, if necessary, further risk treatment. Steps 8 and 9 on the Process Map above describe the Residual Risk calculation process.

ADD-ON COMPONENTS (OPTIONAL)

1. Business Impact Analysis

a. Identify departments that are critical to an organization's business.
b. Document individual departments core processes, system initiatives, and regulatory requirements.
c. Identify what applications are critical to each department and their infrastructure dependencies.
d. Establish recovery point objective (RPO) and recovery time objective (RTO) metrics for each application.
e. Identify what data is being received and processed by each department.
f. Identify internal and external departmental dependencies.

2. System Characterization

a. Identify applications that are critical to the organization's business process and determine application dependencies.
b. Provide a high-level overview of the applications purpose and functionality.
c. Identify and document the supporting infrastructure of the system.
d. Identify any sensitive or regulated data that the system stores, processes, or transmits.

SECURITY HEALTHCHECKS | INTERNAL EVALUATIONS | LOGISTICAL DOCUMENTATION