Risk Advisory Services Solutions

Business Crisis Management and Simulation

Tabletop exercises are active, situational-based sessions designed to test how various individuals and teams in your organization would respond to a cybersecurity incident. All tabletops led by our Advisory Services team are based on current tactics, techniques, and procedures employed by threat actors, as well as perceived gaps in your current incident response plan. These exercises help your organization determine its' maturity in responding to a breach.

The engagement will begin with a kickoff meeting to confirm the scope and objectives, identify client stakeholders, and establish the rules of engagement. Based upon the information discussed and exchanged during the kickoff call, the Advisory Services consultant will collaborate with the client team to design a realistic scenario based upon the client environment. If provided and desired, specific controls, vendors, and internal processes will be designed into the exercise. The Advisory Services consultant will lead the exercise as defined and confirmed by the client. Depending on the client’s requirements, the session can be delivered on-site or remotely.

The exercise will begin with the moderator presenting the team with the initial details of the scenario. The team will be asked to react and respond to the situation. The moderator will guide the team as necessary, encouraging discussion and collaboration. Additional details will be provided as injects to the scenario, progressing the exercise and encouraging more discussion. The exercise will conclude with a roundtable discussion soliciting feedback, thoughts on the exercise, and relevant next steps.

At the conclusion of the engagement, the Advisory Team will develop a detailed written report of the engagement including findings, recommendations, and lessons learned from the engagement. A meeting will be scheduled to review the report with the client.

SPEARTIP

A company of ZURICH

Risk Advisory Services Solutions

Penetration Testing

SpearTip's Penetration Testing adheres to a goal-based methodology, leveraging attacks that emulate adversaries, to demonstrate the risk associated a given client's attack surface.

Penetration Testing exposes security flaws that passive vulnerability scans or assessments cannot. The objective of a Penetration Test is to demonstrate weaknesses in systems or network services and move through the network gaining and expanding access to target systems or data. The test includes exploitation of vulnerabilities, identify and authentication attacks, and lateral movement through compromised hosts.

Testing begins with a kickoff meeting to confirm the scope and objectives, identify client stakeholders, and establish communication and the rules of engagement. The penetration tester will utilize open-source intelligence and technical tools to enumerate the target environment and gather relevant information. The penetration tester will analyze the information gathered to identify potential vulnerabilities and formulate an attack strategy, attempting to exploit identified vulnerabilities and achieve the objectives that were established during the engagement kickoff.

At the conclusion of the engagement, The testing team will develop a detailed report of the engagement including findings, recommended remediation steps, and a detailed narrative of the engagement. A meeting will be scheduled to review the report with the client. All penetration tests include remediation validation for Critical-, and High-Severity issues identified and remediated with 90 days of testing.

Risk Advisory Services Solutions

Vulnerability Assessment

SpearTip's Vulnerability Assessments help determine the overall risk to client assets and digital environments. The vulnerability assessment is an in-depth inspection for security weaknesses by identifying, quantifying, and prioritizing vulnerabilities in the client environment.

The assessment will begin with a kickoff meeting to confirm the scope and objectives, identify client stakeholders, and establish the rules of engagement. The assessor will utilize open-source intelligence and technical tools to enumerate the target environment and gather relevant information. In-scope assets will be scanned using industry-standard cybersecurity vulnerability assessment tools. These tools are designed to identify and classify vulnerabilities, services, and configurations within the environment. The assessor will analyze the scan results and prioritize the findings based on severity, likelihood , and potential impact using the industry-standard Common Vulnerability Scoring System (CVSS).

At the conclusion of the engagement, the Advisory Services team will develop a detailed written report of the engagement including findings and recommendations from the engagement. A meeting will be scheduled to review the report with the client.

Risk Advisory Services Solutions

Cybersecurity Gap Analysis

The Advisory Services Team will conduct an in-depth assessment of your administrative, technical, and physical security controls based on the NIST Cybersecurity Framework (CSF). The assessment will begin with a kickoff meeting to confirm the scope and objectives, identify client stakeholders, and establish the rules of engagement.

The Advisory Services Team will request and review client documentation and schedule interviews with identified client stakeholders. Requested documentation may include written policies and procedures, recent risk assessment reports, and cybersecurity roadmaps. The Advisory Services Team will conduct interviews with client stakeholders to validate, clarify, and address any information gaps in the provided documentation. The Advisory Services Team will assess the client’s security controls against the 22 categories and 106 subcategories of the NIST Cybersecurity Framework (CSF) and formulate recommendations to address control gaps and improve the client’s overall security posture.

At the conclusion of the engagement, The Advisory Services Team will develop a detailed written report of the assessment including findings, benchmarks, target profile and recommendations. A meeting will be scheduled to review the report with the client.

SPEARTIP

A company of ZURICH

Risk Advisory Services Solutions

Cybersecurity Health Check

The Advisory Services Team will conduct a foundational assessment of your administrative, technical, and physical security controls based on the NIST Cybersecurity Framework (CSF).

The assessment will begin with a kickoff meeting to confirm the scope and objectives, identify client stakeholders, and establish the rules of engagement. The Advisory Services Team will request and review client documentation and schedule interviews with identified client stakeholders. Requested documentation may include written policies and procedures, recent risk assessment reports, and cybersecurity roadmaps.

The Advisory Services Team will conduct interviews with client stakeholders to validate, clarify, and address any information gaps in the provided documentation. The Advisory Services Team will assess the client’s security controls against the 22 categories of the NIST Cybersecurity Framework (CSF) and formulate recommendations to address control gaps and improve the client’s overall security posture.

At the conclusion of the engagement, the Advisory Services Team will develop a detailed written report of the assessment findings and recommendations. A meeting will be scheduled to review the report with the client.

☎ **Breach Response**
833.997.7327

Emergency: breachresponse@speartip.com
Non-Emergency: info@speartip.com