Scope of Work

The following will describe the scope of work for each service:

Penetration Assessment Services

SPRWS seeks a qualified firm to conduct comprehensive cyber and physical penetration assessments of its assets, identifying vulnerabilities from both internal and external attack vectors. This high-level scope of the testing project includes the following tasks and deliverables:

Tasks:

Red Team Assessments:

- **Annual Testing to include as needed and specified by each statement of work:**
  - **Internal Testing**: Assess internal systems and networks for vulnerabilities.
  - **External Testing**: Evaluate external interfaces and web applications for security weaknesses.
  - **Web Application:**
  - **Social Engineering**: Conduct assessments to identify susceptibility to social engineering attacks.
  - **Remediation Validation**: Verify the effectiveness of remediation efforts from the previous assessment.
  - **Remediation Validation**: Validate remediation efforts from the previous Q1 assessment.

Blue Team Engagement:

- **Proactive and Reactive Defense**: Leverage human intelligence with tools and technologies to enhance security posture.
  - **Incident Response**: Develop and refine incident response strategies.
  - **Defensive Security**: Implement measures to protect against and respond to threats.
  - **Infrastructure Protections**: Ensure robust defenses for critical infrastructure.
  - **Damage Control**: Develop strategies to mitigate damage in the event of a breach.
  - **Operational Security**: Maintain security protocols and procedures.
  - **Threat Hunting**: Proactively search for signs of malicious activity.
  - **Digital Forensics**: Analyze incidents to understand and learn from breaches.

Deliverables:

- **Requirements Documentation**
- **Final Design**
- **Timeline**
- **Executive Summary**
  - Overview of the project and key findings.
  - Strategic recommendations for remediation efforts.

RB Advisory LLC
163 E Morse Blvd, Suite 220
Winter Park, FL 32789

- **Findings Report**
  - Detailed technical report outlining vulnerabilities discovered.
  - Severity ratings (Critical/High/Medium/Low/Informational) for each finding.
  - Assessment of the level of effort required for exploitation.
- **Recommendations**
  - Actionable remediation strategies for each disclosed finding.
  - Guidance on industry-leading best practices to enhance security posture.

RBA's Cyber Security Program Assessments

RBA'S cyber security program assessment approach is designed to meet the needs of state and local government organizations. The approach builds on the standards and best practices promoted by NIST, the Department of Homeland Security and various other government and industry groups. RBA brings substantial additional insight and value to these standards based on our decades of experience working with government teams to design and execute successful performance improvement plans.

The result is a methodology that identifies your organization's most critical needs, prioritizes those needs in a meaningful way, and sets out a detailed plan to meet those needs that is tailored to the unique structure and capabilities of your organization.

A Holistic View of Your Cyber Security Program

RBA has identified seven elements of a successful cyber security program. Like the proverbial weak link in a chain, if any one of these elements is missing or immature, the effectiveness of your entire program is in jeopardy. Our security analysts evaluate each of these Eight elements against industry standards, compliance needs and known points of failure.

RB Advisory LLC
163 E Morse Blvd, Suite 220
Winter Park, FL 32789

Risk Management: Are there processes in place and followed to identify critical assets and their threat exposure?

Governance: Are up-to-date policies and procedures monitored and enforced to ensure cyber security best practices are followed across the organization?

Security Organization: Is there a team in place with the skills needed to protect the organization's information assets?

Security Tools: Are hardware and software technologies in place to protect assets, notify the team of potential threats and support proactive incident response?

Third Party Risk: Are vendors and service providers incorporated in the cyber security program and are the associated risks of their systems and connectivity understood and documented?

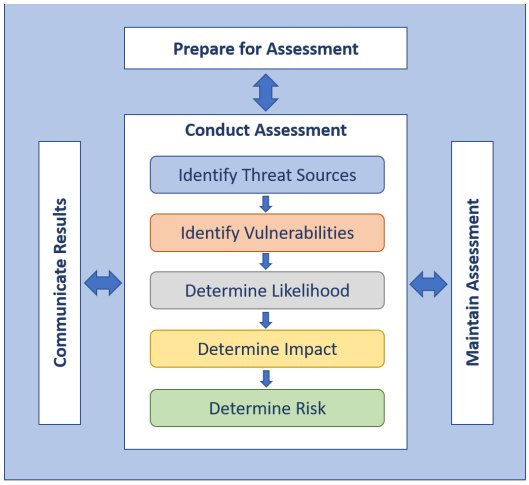
Threat Management: Are the tools in place to ensure the team always has refreshed threat insight data and understands how to monitor and respond to changes in the threat environment?

Incident Response: Is there a robust plan with adequate training to ensure the organization can quickly respond to any suspected or verified breaches to minimize potential damage and resume normal operations as quickly as possible?

Risk Assessment

Risk assessment is a key component of the Identify function in the CSF. It is a fundamental, iterative activity that is part of the foundation of a sound and effective security framework. Properly implemented risk assessments produce a prioritized inventory of the threats faced by an organization. They enable the organization to develop effective plans to mitigate threats and roadmaps to a more secure future.

RB Advisory LLC
163 E Morse Blvd, Suite 220
Winter Park, FL 32789



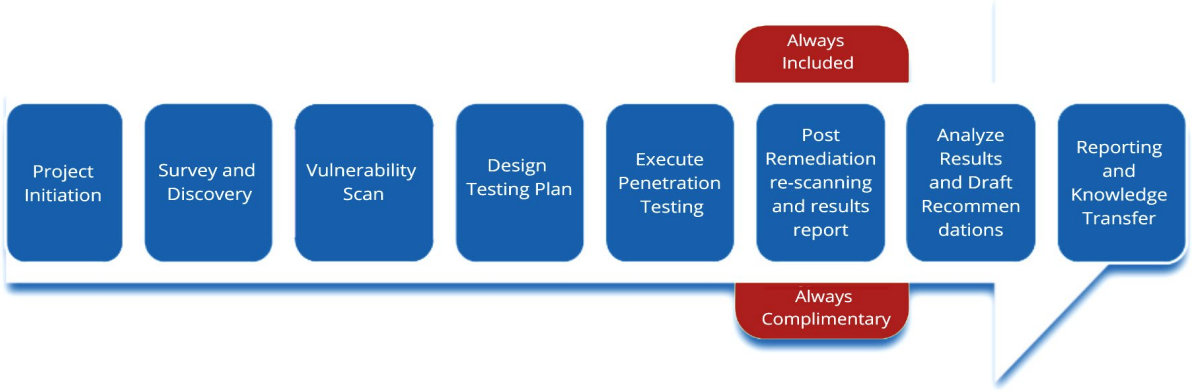
The Risk Assessment Process
Adapted from NIST 800-30

NIST publication 800-30 provides guidance for conducting risk assessments. RB ADVISORY has developed a methodology that embraces the 800-30 guidance and enhances it based on our extensive experience working with public sector institutions of all sizes and missions.

- **Identification of Threat Sources and Events**
  Understand what threat sources are relevant and not, to the context of the organization, as well as what the associated threat event could be.
- **Identification of Vulnerabilities and Predisposing Conditions**
  Understand administrative, managerial, procedural, and technical vulnerabilities within the organization that could be exploited through defined threat sources as well as the current predisposing conditions that could lead to a successful exploitation.
- **Determination of Likelihood of Occurrence**
  Define the likelihood that the identified threat sources would execute certain threat events and the likelihood of these events being successful.
- **Determination of Magnitude of Impact**
  Define the business impact to organizational assets, individuals, related organizations, and ultimately the nation, as a result of a vulnerability exploitation.
- **Final Determination of Organization Risk**
  Determine the overall information security risks as a combination of the likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with risk determinations.

RB Advisory LLC
163 E Morse Blvd, Suite 220
Winter Park, FL 32789

RBA's Penetration Test Methodology



BEST PRACTICES IMPLEMENTATION

Our team utilizes multiple recognized Information Security best practices and standards while providing services to our clients. Some of the main standards include:

- IEC/ISO 27000 Series (Security Management and Control).
- National Institute of Standards and Technology (NIST) – Computer Security Standards.
- SANS Institute Guidance – Testing Methodologies and Approaches.
- Open Web Application Security Project (OWASP) – Web Application Testing and Assessment.
- Open-Source Security Testing Methodology Manual (OSSTMM) – Methodology for performing security tests and metrics.
- Payment Card Industry Data Security Standard (PCI-DSS).
- Information Systems Security Assessment Framework (ISSAF) – Methodology for information system security assessments.
- Penetration Testing Framework v0.58 – Community updated penetration testing framework.

ACTIONS / APPROACH

Our assessments are conducted with the use of both non-intrusive and robust commercial scanning tools and manual tests by our team of experts who will provide comprehensive infrastructure reports of active IP systems. When necessary, open-source tools are used to validate certain checks to remove any false positives.

RB Advisory LLC
163 E Morse Blvd, Suite 220
Winter Park, FL 32789

NETWORK PENETRATION TESTING METHODOLOGY

Multi-Stage Attacks

Our assessment methodology incorporates the use of NIST 800-115, "Technical Guide to Information Security Testing and Assessment" which requires escalation procedures in which the assessment seeks to determine the likelihood that risk associated with single foothold in an environment will be compounded through lateral advance and chaining separate attack techniques in order to escalate privileges with the goal of compromising beyond the initial foothold.

During our assessments, we perform a threat vector assessment through manual and automated reconnaissance of the network. Through prioritizing the potential risks associated with misconfigurations, and known vulnerabilities identified through reconnaissance, we manually validate each threat vector with the goal of exploiting the misconfiguration or vulnerability to gain unauthenticated access to the target system.

We then execute various multi-staged attacks against the application, OS, and/or network stack in support of the compromised system in order to move laterally throughout the network and leveraging access tokens (credentials) against other systems. Throughout the development of our "Attack-Chain" we document the initial foothold, and subsequent techniques used to parlay our initial access into an escalated state. The use of multi-stage attacks to escalate privileges is key to understanding the risk and mitigating controls in place to minimize the likelihood threat vectors can be used to compromise the confidentiality, availability, or integrity of systems.

Check and Balances

Our assessment methodology is based on risk determination guidance contained within NIST 800-115. We understand that our assessors have limited time to identify and validate misconfigurations or vulnerabilities that exist within the environment. Given the threat identification process is a dynamic and continual process, there is no reasonable expectation that all threat vectors will be identified or exploited during our assessments.

In order to ensure that the most "likely" attacks are covered, our threat vectorization stage is performed to identify vulnerabilities and misconfigurations that present the most likely risk given the level of difficulty and prevalence of the issue within the constraints of the scope of the assessment. All weaknesses that are identified are assumed to be repeatable by malicious actors given the same level of expertise and time against the system.

Our methodology thus prioritizes the most serious "low-hanging fruit" for inclusion in testing to validate these weaknesses and ensure the organization is reducing threat surface proportionally (given resource constraints) during the remediation process. All weaknesses

RB Advisory LLC
163 E Morse Blvd, Suite 220
Winter Park, FL 32789

identified during our assessment are also weighed against and manually validated for their likely use in "multi-stage" attacks further in a potential the attack-chain. We give priority to misconfigurations and vulnerabilities that are known to be key leverage points for lateral advance and privilege escalation as these inherently carry more overall risk to the environment than other weaknesses that are systemic to an application, platform, or network.

Elimination of False Positives/Negatives

Our methodology is based on guidance contained within NIST 800-115 as it relates to verification and validation of a potential weakness. The identification of a "potential" weakness during our reconnaissance and threat vectorization phase provide context to our chosen attack-paths and not create specific reportable weaknesses directly. In this way, our methodology inherently removes false-negatives and false-positives form the reporting phase due to our requirement to validate and re-perform exploitation of the misconfigurations or vulnerabilities in order to diagnose the potential level of lateral advance or privilege escalation associated with the weakness.

Our methodology also includes procedures for continual feedback and management awareness of assessment risks when the assessment's scope is non-evasive. If during our threat vectorization phase, we identify a potential weakness that may create availability concerns or network operational harm if exploited, our team will raise client awareness of the issue and validate the concern through non-destructive measures (e.g., obtaining diagnostic information from the system, which cannot be observed from the assessor's scope). This procedure further increases the level of integrity contained within the final reported weaknesses and ensures that potential false positives/negatives are minimized if not completely avoided.

SOFTWARE/TOOLS

Our choice of tools and techniques will enable us to identify and map network devices, to determine if the IT infrastructure services implement security measures sufficient to protect sensitive information. Our choice of VA scanning tools combined with the knowledge of our expert penetration testers and risk assessors will help to determine the level of security and evaluate how vulnerable the identified systems are to potential system attacks, penetration, and information loss due to external hacker threats or internal malicious/curious network usage.

We conduct our testing using recognized frameworks such as OSSTMM[1], PTES[2], and NIST[3]. Our consultants are authorized, trained, and licensed to use the following commercial packages as well as other popular solutions, all driven by project requirements:

- Open-Source Intelligence (OSINT)

[1] Open-Source Security Testing Methodology Manual (http://www.isecom.org/research/osstmm.html)
[2] Penetration Testing Execution Standard (http://www.pentest-standard.org/index.php/Main_Page)
[3] National Institute of Standards and Technology (http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf)

RB Advisory LLC
163 E Morse Blvd, Suite 220
Winter Park, FL 32789

- SAINT Scanner/Exploit (www.saintcorporation.com).
- BurpSuite Pro (http://portswigger.net/burp/).
- Nessus (www.nessus.org).
- Cobalt Strike (www.advancedpentest.com).
- Acunetix Web Application Security (www.acunetix.com).
    - In addition to the commercial software, the following open-source tools/distributions will be used, as required:
- **Kali 1.x** – Linux distribution aimed at penetration testing and digital forensics. These toolkits include a wide range of software to aid a tester in testing networks and applications for vulnerabilities and using the results to penetrate a network. Kali contains a wide variety of open-source tools for use during penetration testing including:
- MetaSploit Framework.
- BurpSuite.
- w3af – open-source web application security scanner.
- nmap.
- CSRFTester.
- WebScarab.
- **Samaurai** – a live Linux environment that has been pre-configured to function as a web pen-testing environment. While similar to the BackTrack distribution, this framework focuses on Web Application testing.

RB Advisory LLC
163 E Morse Blvd, Suite 220
Winter Park, FL 32789