



THE RISK

In today's business environment, there is an increasing demand for organizations to become more secure and accountable. With the help of the media and lawmakers, businesses are quickly noticing that security breaches and privacy concerns are becoming common occurrences. Regulations are forcing organizations to recognize and secure their vulnerabilities.

THE SOLUTION

The Rapid Risk Assessment is an effective way of identifying current risks and establishing (or validating) an information security roadmap for the organization. The assessment will deliver a comprehensive report identifying the critical vulnerabilities within the organization and associated recommendations for remediation. Remington's Rapid Risk Assessment services, based on ISO 17799, a globally recognized set of information security standards, is available in five varieties.

Remington's Rapid Risk Assessments:

- Risk Discovery (ISO 17799 gap analysis)
- Legal Liabilities Analysis
- SDLC Assessment
- External Vulnerability Testing
- Ethical Hacking



RISK DISCOVERY

The Risk Discovery process takes a few days to perform for most organizations and consists mainly of interviews with key personnel. The assessment covers all 11 domains of ISO 17799.

Areas of Coverage *(ISO 17799 Domains - June, 2005 Version)*

- Security Policies
- Organizing Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance



Benefits

- Provides clear picture of current risks as well as underlying source(s)
- Directs focus of organization to key areas of risk
- Demonstrates due diligence
- Provides justification for information security controls, resources and audits
- May fulfill prerequisite for cyber insurance

Deliverables

- Comprehensive findings report based on ISO 17799
- Details of identified security strengths and weaknesses with associated liabilities
- Prioritized list of recommendations to remedy identified risks
- Supporting best practices, standards and frameworks as appropriate



LEGAL LIABILITIES ANALYSIS

Three types of legal liabilities exist within information security: **direct-legal liability**, **indirect-legal liability** and **non-legal liability**. Remington Associates and its legal partners will help you understand what liabilities may exist as a result of the vulnerabilities in your organization's information systems, employee policies, contracts, privacy statements and handling of private data or intellectual property.

Areas of Coverage

- Identify applicable laws, regulations and corresponding organizational security requirements
- Determine scope of confidential and private information
- Determine categories of intellectual property to be protected
- Review existing contracts and confidentiality agreements, specifically concerning third parties
- Review insurance policies to determine coverage for security and privacy issues
- Review asset and data classification policy
- Review information security policies, employee policies and current allocation of security roles and responsibilities
- Review terms and conditions of employment, including information security responsibilities, training, and incident reporting procedures
- Evaluate record retention policies and practices
- Review privacy statements
- Correlate results of technical assessments with legal liabilities

Benefits

- Understand legal liabilities
- Obtain a list of recommended mitigating controls
- Identify recommended changes to agreements, policies and procedures

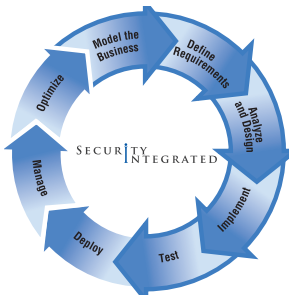


SDLC ASSESSMENT

Software applications (custom or purchased) provide access to the core assets and processes within the organization. The Systems Development Life Cycle Assessment will look at each stage of the SDLC to ensure that unnecessary risks are not introduced into the business. Our security specialists will then make recommendations to ensure best practices are met.

Areas of Coverage

- Applicable regulations requirements
- Security requirements including mis-use cases
- Traceability of requirements throughout the SDLC
- Use of appropriate identity and access management
- Proper use of session management
- Database security configuration
- Defensive coding techniques to prevent vulnerabilities
- Security validation techniques
- Appropriate use of automated testing tools (for load, function and security testing)
- Current assignments of security roles and responsibilities
- Adequate use of other best practices and standards



Tasks To Be Performed

- Interview key members of the development team and business sponsors
- Review any available artifacts (requirements, design, test plans, etc.)
- Review application architecture and database design
- Correlate vulnerabilities with lack of specific best practices
- Provide best practices training and guidance for establishing and maintaining a secure SDLC

Benefits

- Understand the source of identified Web application vulnerabilities
- Receive expert recommendations for remediation of identified vulnerabilities
- Understand best practices, methods and techniques to incorporate into the SDLC

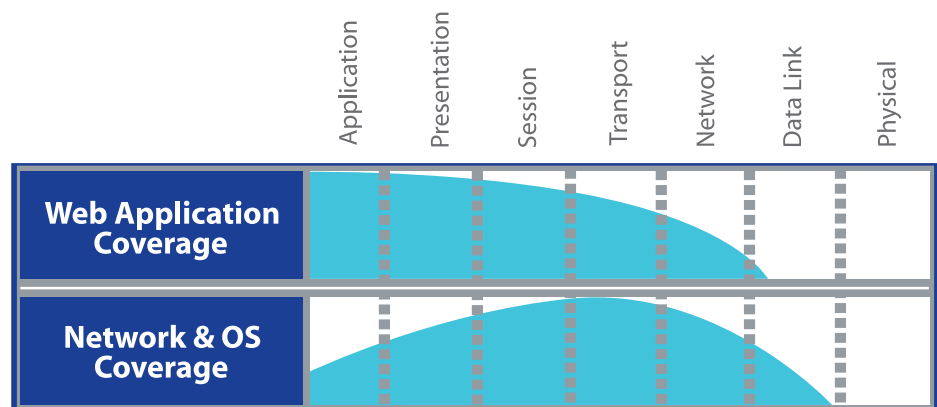


EXTERNAL VULNERABILITY TESTING

External Vulnerability Testing may be applied to any Internet-accessible system or Web application. The primary objective is to identify obvious vulnerabilities that would make the organization a target of attack from malicious Internet users. Many less-skilled hackers will pursue the easy targets, commonly referred to as the “low-hanging fruit.” By scanning for systems with common vulnerabilities and signs of poor security management, they focus on a very small fraction of all the systems on the Internet. The main objective of this assessment is to help identify the essential steps that should be taken in order to ensure that your systems do not appear to be “low-hanging fruit.”

Tasks To Be Performed

- Vulnerability scanning using automated tools
- Identification of patterns and evaluation of associated risks
- Manual testing of systems and services, with focus on key reported vulnerabilities
- Recommendations for remediation of identified vulnerabilities





ETHICAL HACKING

Ethical Hacking utilizes the recon delivered from automated scans, combined with the efforts of experienced ethical hackers in order to penetrate the organization's perimeter and its Web applications. The goal of Remington's Red Team is to gain access and control of targeted systems. Reports will include documented penetration scenarios as well as detailed recommendations for remediation.

Tasks To Be Performed

- Scan systems using manual recon methods as well as automated tools
- Review scans to rule out "false positives"
- Develop a plan of attack
- Attempt to compromise system permissions and escalate privileges through programmatic manipulation
- Upload and execute programs to exploit discovered vulnerabilities
- Report findings with infiltration scenarios
- Provide recommendations for remediation



Network & OS

Web Applications

External Vulnerability Testing	Scanning and verification of Internet-accessible hosts	Scanning and verification of Web applications
Ethical Hacking	Manual penetration testing of Internet-accessible services	Manual penetration testing of Web applications



REMINGTON ASSOCIATES, LTD.
 SECURITY INTEGRATED