WHAT ARE RISK ASSESSMENTS

Risk assessments are essential activities performed on your company's security infrastructure that reveal threats to key corporate assets and vulnerabilities in your current security controls. The ultimate goal of a risk assessment is to define appropriate safeguards tailored to your company's risk profile and priorities. Risk assessments usually precede and help define audit plans and facilitate the development of a corporate security plan. An IS auditor performs a risk assessment to provide reasonable assurance that all material items will be adequately covered during the audit.

Risk assessments have multiple components and can include security reviews, gap analysis and any number of tests and diagnostics to assess various areas of the security framework. Complete risk assessments will include most of the following components depending on the specific needs of the customer. Each component has separate goals and a different process, but all are designed to identify vulnerabilities and to assign a probability of occurrence so that a plan can be defined related to controlling that risk.

Risk Assessment Components

❶ **Security Review & Gap Analysis**		Audit your security strategy, architecture and controls and determine if they are appropriate to protect your key digital assets.
❷ **Security Tests**		Security Tests diagnose actual vulnerabilities by testing specific areas of your security infrastructure.
Security Tests	**Network Vulnerability Tests:** • **External & Internal**	Automated tests applied from outside & inside your network to identify basic vulnerabilities to common current threats. Internal scanning looks at all endpoints and network devices for risks.
	Network Penetration Tests • **Internal & External Tests**	**Targeted** attacks on your network by **white hat hackers** looking for vulnerabilities to sophisticated attacks from the inside or outside your Network
	Web Application Penetration	A rigorous testing process that includes a series of fabricated malicious attacks to see the level of security of the Web application system
	Social Engineering Tests	Pretending to be a trusted party to manipulate an authorized user to provide access to confidential business secrets or information about usernames and passwords (frequently Phishing exploits).
	Wi-Fi Review & Testing	Examines the security of the wireless topology and design. Wireless components such as controllers, access points, client workstations and mobile device settings are reviewed to ensure proper security measures
	VOIP Testing	
	Security Configuration	Examines the security features and settings of IDS, IPS, UTM security appliances and other security solutions for optimal security configurations.
	Operational Tests	Selected tests of various corporate systems for security controls such as application software tests.
	Physical Security Tests	Testing of physical and environmental infrastructure for appropriate security controls for office and data centers and vulnerability to environmental disasters.
	3rd Party Vendor Reviews	Review 3rd party business associates for compliance with your security standards or with Security regulations.

Who Needs Risk Assessments -- Why are They Important

There are three important reasons why companies need risk assessments:

1. **All companies need to use risk assessments as a proactive effort to discover where the current security risks are in your businesses.** Risk assessments are important because they protect your company's IP and financial data as well as your customer's and business partner's data. Once a risk assessment is complete, making decisions about how to prioritize short term risk mitigation expenditures is much more informed. Special actions can be taken to reduce risks from identifiable threats and vulnerabilities. The ability to develop a security strategy come directly from the results of a risk assessment.
2. **Risk assessments are also an essential part of the security regulation compliance process.** Security regulations such as PCI/DSS, HIPAA, SOX, NIST, financial regulations, GDPR and others all require a security risk assessment as step one to

become compliant. Regulated companies and companies whose customers are regulated will need to do risk assessments to avoid breaches, fines and other penalties like not being able to continue to sell to their customers.

3. **A third reason to use a risk assessment would be in response to a security breach or attempted breach.** Risk assessments can take a wholistic approach to evaluating your security posture and to focus in on potential areas of weakness. Once complete, a more strategic approach to future security investments can be made so that you can avoid future breaches.

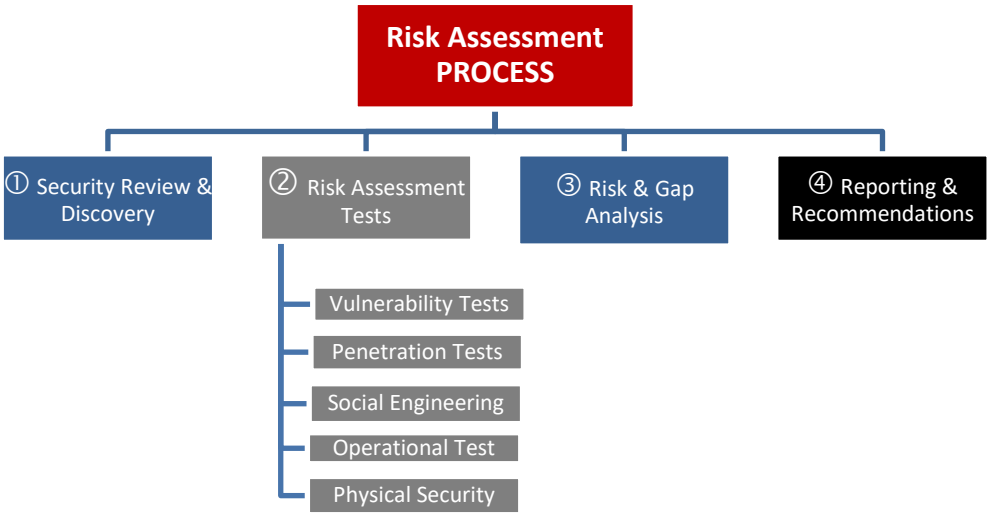
RISK ASSESSMENT ALTERNATIVES

Risk assessments are a complete process for understanding your businesses risk posture so that a security strategy can be put in place or updated and to generate security remediation plans to address the company's highest risks. To do that, an auditor must implement a process of discovery and analysis that includes a thorough understanding of your business, *risk assessment tests*, analysis and reporting on findings and recommendations.

	RISK ASSESSMENT / AUDIT OPTIONS			
Risk Assessment Process Steps	❶ **Security Review & Gap Analysis**	❷ **Core Risk Assessment**	❸ **Advanced Risk Assessment**	❹ **Functional Tests**
	CORE REVIEW	**BETTER**	**BEST**	**SELECT**
1. Security Review & Discovery • Complete set of interviews and fact finding • See process description for detail	X	X	X	
2. Perform Risk Tests				
A. Ext. & Internal Network VULNERABILITY Tests		X	X	Opt
B. Ext. & Internal Network PENETRATION Tests		Opt	X	Opt
C. **Web Application Penetration Testing**			X	Opt
D. **Social Engineering Tests (Phishing & Other)**			X	Opt
E. **Wi-Fi Penetration Testing**			X	Opt
F. Security Configuration Testing and Analysis			Opt	Opt
G. Physical Security Tests			Opt	Opt
H. VOIP or Other Tests			Opt	Opt
3. Risk & Gap Analysis • Determine Risk Areas & Prioritize based upon level of discovery and tests performed • Define Prioritized Remediation Alternatives	X	X	X	
4. Report & Management discussion re: findings and recommendations	X	X	X	
5. Remediation implementation (Security consulting to implement or configure new products, current products, policies or procedures) **[To be quoted after initial risk assessment]**	Opt	Opt	Opt	Opt
Employee awareness training & education	Opt	Opt	Opt	Opt
Quarterly or Annual Follow-up & retest	Quote	Quote	Quote	Quote

RISK ASSESSMENT PROCESS

The risk assessment process is designed to provide complete end to end fact finding, testing, analysis and reporting. The goal is to completely analyze all components necessary to provide an understanding of risks, gaps and recommendations. Refer to the previous and following charts to see how each task fits within the overall risk assessment project.



1. **Security Review & Discovery**
    a. Management & technical Interviews as appropriate
    b. Understand your business objectives
    c. Determine your key digital assets to protect
    d. Review security strategy
    e. Review organization, security architecture, systems, IT plans
    f. Review your current security controls
    g. Review your security related policies and procedures
    h. Compliance level review & review of prior external audit findings
2. **Perform Risk Tests** including <u>any or all</u> of the following (**OPTIONAL TESTS**):
    a. Vulnerability Testing:
        i. External vulnerability testing
        ii. Internal network vulnerability testing
    b. **Configuration & Implementation analysis** of selected security controls that are in place
    c. Detailed Analysis of Policies, Procedures and Duties
    d. **Penetration (Hacker Tests)**
        i. External network
        ii. External Web application (website)
        iii. Internal network penetration testing
        iv. Wi-Fi penetration tests
    e. Operational tests:
        i. Social engineering
            1. Email phishing
            2. Non-email social engineering tests
        ii. Physical security etc. (Optional)
        iii. VIOP system testing
    f. Hacker Safe Tests: External penetration tests (Optional)
3. **Risk & Gap Analysis:**
    a. Analyze Findings
    b. Determine likely risks and probability of occurrence
    c. Develop risk mitigation alternatives & recommendations
4. **Generate Report & Discussion risks with your management team**
5. **Optionally Retest After Mitigation Efforts Applied & Revise Report**

RISK ASSESSMENT COMPONENTS

Security Review & Gap Analysis

The most important part of the suite of components in the risk assessment process is clearly the Security Review & Gap Analysis. It is the glue that ties the entire risk assessment solution set together. As with a security audit, there must be a process for assessing a company's risk profile. While it is possible to run specific tests to assess specific security vulnerabilities, understanding a company's overall security posture is also important.

A security Review and Gap Analysis' purpose is to audit your security strategy, architecture and controls and determine if they are appropriate to protect your key digital assets. This may be the most important first step in security assurance. The process used leverages our extensive experience in security in understanding your business, key assets, how and who access your data and what controls you have and should have in place to protect your assets. Process steps include:

- Security Review & Discovery
- Risk & Gap Analysis
- Recommendations
- Reporting

While this assessment process can be done without the execution of any other tests, it will lack key test data on your security systems and vulnerabilities with those tests. As a result, it is recommended that the review and gap analysis is done in conjunction with other high value tests such as vulnerability scans and penetration tests.

The results of the review and gap analysis is a prioritized list of vulnerabilities and recommendations based upon the information you have provided. By adding other tests, we can use those test results to provide actual real-world vulnerability information into your analysis. Regardless of whether other tests are performed, the value in having someone outside your company who are experts in security reviewing your security posture is immense and should be performed annually if possible.

Network Vulnerability Scans

Vulnerability scan tests are partially automated tests that can be run internally or externally to your network to discover vulnerabilities at your gateway or internally on your endpoints. These tests are best performed by a security expert so the interpretation of the results provides appropriate remediation actions and priorities.

External Vulnerability Scans

External vulnerability scans are run from an external data center examining your externally facing IP addresses looking for exposed firewalls, Web servers and other publicly facing devices. These tests expose easy to exploit vulnerabilities by hackers and are typically required to be compliant with most security regulations such as PCI, HIPAA and financial.

Internal Vulnerability Scans

Internal vulnerability scans inspect networks from the inside looking at all endpoints and network devices for risks. These tests provide in-depth testing of each scanned device in your network looking for device vulnerabilities. Since roughly 50% of threats occur from the inside, it is essential to test your network both externally and internally.

Why do you need some type of vulnerability scan for your network and devices?

- ☑ **To be compliant with most security regulations**
  - PCI: Quarterly External Scans
  - Health, Financial and Privacy Regulations
- ☑ **Vulnerability scans are an essential part of any security audit**
- ☑ **Increase your security by providing automated auditing of:**
  - Asset Inventory (What is attached to your Network)
  - Mobile Devices
  - Botnet/Malicious Process/Antivirus
  - Patch Management Systems (Verifies applied patches against patch management systems) - Optional
  - Sensitive Content (credit card, financial, personal, copy-written and other types)

Network Penetration Tests

Many companies must need to, or want to, perform aggressive testing of their externally facing network (the Internet gateway) to see if targeted attacks can penetrate the internal network. Penetration Testing, also known as ethical hacking, are conducted to determine the true risk of vulnerabilities identified through exploitation of vulnerable externally facing

network devices. These attacks attempt to gain root or administrator-level access to target systems or other trusted user account access. At least two types of penetration tests can be performed. Website and Web application testing examines externally facing Websites and the highly vulnerable operating systems, Web servers, databases and custom applications running on these servers. These tests must be implemented by highly trained security white hat hackers.

Internal and External Network Penetration Tests
These tests are focused on penetrating your Internet gateway and the security provided at that location. It will test for vulnerabilities to firewalls, routers or any externally facing network devices and any systems behind it that can be accessed from outside your network. Ethical hackers will apply current hacking attacks and targeted attacks to see if your network can be penetrated. This testing includes automated external vulnerability scans but goes far beyond by attacking with white hat state of the art hacking attacks.

Website and Web Application Testing

Web applications are a major point of vulnerability in organizations today. Web application security holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited Web sites altered by attackers.

Securing a company's customer private data and network, and regular risk assessments are part of almost every security regulation. Merchant security's PCI DSS Requirement 11.3 obligates organizations that process, store, or transport credit card data to implement a methodology for web application penetration testing. This is a recurring commitment—not one and done. This testing must be performed when there is significant change and at least yearly. Merchants as well as payment processors, financial institutions and service providers share this responsibility.

Typically, Web application security testing is performed after the Web application is developed. The Web application undergoes a rigorous testing process that includes a series of fabricated malicious attacks to see how well the Web application performs/responds. The overall security testing process is followed by a format report that includes the identified vulnerabilities, possible threats and recommendations for overcoming the security shortfalls.
Some of the processes within the testing process include:

- Brute force attack testing
- Password quality rules
- Session cookies
- User authorization processes
- SQL injection

Social Engineering

'Social Engineering' is a threat, often overlooked but regularly exploited; to take advantage of what has long been considered the 'weakest link' in the security chain of an organization – the 'human factor'. "Social engineering is the practice of obtaining confidential information by manipulation of legitimate users.

A social engineer will commonly use the telephone or Internet to trick a person into revealing sensitive information or getting them to do something that is against typical policies. Hackers often use phishing or emails with phony links in them to get users to go to what they think is a friendly Website and enter their user name, password and other private information. Instead that information is going to the hackers for later use.

By using these methods, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. It is generally agreed upon that "users are the weak link" in security and this principle is what makes social engineering possible.

Configuration Testing

This review examines the security features and settings of the customers' intrusion detection systems, intrusion protection systems, unified threat management and next generation security appliances for optimal security configurations. Components reviewed include the firewall rule set, threat policy configuration and protection settings, and antivirus/malware configuration and protection settings. Findings will be documented and will include recommendations.

Wireless (Wi-Fi) Architecture Review & Penetration Testing

This review examines the security aspects of the wireless topology and design—with the goal of determining the best possible security posture. Wireless components such as controllers, access points, client workstations and mobile device settings are reviewed to ensure proper security measures have been implemented. And wireless technology is reviewed for best use of security features and capabilities. Recommendations for securing the environment—and applying new technologies and capabilities to enhance security—are documented and included.

Wireless Penetration testing involves physically scanning the perimeter of a facility using a wireless scanner. The wireless scanner probes the general vicinity for any emitted Wireless Access Point (WAP) signals that are in the area. Each responding signal is documented for ownership, whether or not it is a known corporate resource, and whether or not it is secured with encryption. Testing begins within the vicinity of wireless signal(s). Using a commercial laptop outfitted with a special wireless antenna, signals are then collected and identified for ownership. Signals identified as the wireless system belonging to the customer are then targeted for penetration. The attempt to penetrate begins with initiating a request and response from the WAP. As users connect to the device, encrypted packets of information are captured. Depending on the encryption technology securing the wireless network, the number of packets being collected will vary. The packets collected are then examined with an attempt to decrypt them. If successful, the decrypted packets should provide the information needed to connect to the wireless network.

VOIP Testing

This testing consists of dialing a range of phone numbers that belong to the customer. Each phone number is dialed and then monitored for a response. Responding phone numbers that are connected to computer modems and network equipment are documented; a limited exploit is used to determine whether the phone numbers in question belong to the customer, and whether they pose any vulnerability. For customers who have deployed Voice over Internet Protocol Systems (VoIP), this assessment involves identification of the specific VoIP hardware chosen and evaluates it for known security issues. This evaluation will confirm that the proper security settings have been chosen. Using a variety of assessment tools, the employment and functionality in the live environment will be confirmed. Testing of encryption will be accomplished by attempting to intercept audible VoIP packets. Lastly, all the VoIP hardware will be scanned during the normal security analysis of all devices on the network. Suggestions to mitigate exposed risks will be included in our report.

Physical Security

Physical security is an often-overlooked component of data and system security in the technology world. While frequently forgotten, it is no less critical than timely patches, appropriate password policies, and proper user permissions. You can have the most hardened servers and network but that doesn't make the slightest difference if someone can gain direct access to a keyboard or, worse yet, march your hardware right out the door.

Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple layers of interdependent systems which include CCTV surveillance, security guards, protective barriers, locks, access control protocols, and many other techniques.

Summary

Risk assessments are an essential part of security. They are required by every security compliance regulation and required for a secure environment. There are many possible tests that can be applied to test your environment depending on your company's needs. By working with a security expert, you can define which tests should be performed on your business and how often. Since most tests are momentary snapshot of your security posture, they need to be repeated at some frequency such as quarterly to maintain a current view of vulnerabilities. By performing risk assessments as part of an audit, you can get a more complete picture of your security profile and have the information necessary to define a complete security strategy, priorities, budget and longer-term mitigation plan.