

# Risk Assessment

## *Who Needs a Risk Assessment?*

If you are a covered entity according to the Sarbanes-Oxley, GLBA, or HIPAA regulations, you are required to identify reasonable foreseeable internal and external risks to the security, confidentiality, and integrity of nonpublic customer or patient information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.



## *What Makes Our Process Unique?*

Our Risk Assessment is unique in that it goes far beyond the reporting function. We take it further by presenting you with a project management tool that includes a list of recommendations to be used in an overall Gap Analysis. We identify threats, the severity of the threats, and the resources required to remediate vulnerabilities so that your action plan can produce an effective level of security. Recommendations are prioritized so that you can take a first-things-first approach to addressing identified vulnerabilities, allowing you to establish acceptable risk.

## *Project Management is the Key!*



The first step in any good project plan is to determine your current position. Our vulnerability matrix acts as more than a Gap Analysis. It is a project plan that allows your team to effectively implement remediation activities with a top-down, risk-based approach. We provide tools including critical path analysis, resource planning, budgeting, and status benchmarks. They allow management to easily check the status of risk mitigation without having to learn technicalities. The end result is that all members of your team start from, and remain on, the same page. This is critical as you have a limited period of time to achieve compliance with limited resources.

**Start Where You Are: The question is not how to comply to regulations, but how to leverage existing technology and teamwork to make compliance a winning proposition.**

# Security is a maze of information, technology and regulations!

## *What is an Adequate Risk Assessment?*

We believe in a four-pronged approach to risk assessment covering administrative, physical, and technical issues:

- Policy/Procedure Review against FFIEC or HIPAA requirements as per the myriad of booklets and workprograms available.
- Perimeter Testing that goes beyond the “capture-the-flag” mentality to document all vulnerabilities inherent in your existing system.
- Internal Network Scan which mimics attack methods utilized by insiders as well as hackers that have breached your perimeter.
- Social Engineering, Physical Breach Attempts, and Password File Analysis to provide valuable information for awareness training and enlisting user cooperation.

## *That’s the Beginning, Not the End!*

Our risk assessment is a journey and the starting point for your Security Management Process. Once we have identified, documented, and confirmed the vulnerabilities, we then analyze them from the perspective of risk-level, threat-level, and resources required for remediation. We produce an executive summary report that addresses management issues such as overall system condition, budget issues, critical path remediation strategy, and the vulnerability matrix. Security is often perceived as a cost.



Our team helps you manage the entire security management process. Our matrix includes an index developed to assist your team on the important risk management issue of prioritization. This algorithm helps your remediation team benchmark progress over time. It organizes the report with the highest-risk, easiest-to-fix vulnerabilities at the top and the lowest-risk, hardest-to-fix vulnerabilities at the bottom. Thus, you can start your compliance project in a first-things-first prioritized manner. Technical information is provided (in CD format) so that your technicians can drill down for more details when necessary.

## *Security Awareness Training*

We recommend that awareness training be one of your first milestones. When all persons associated with your financial institution understand information security, your compliance path gains momentum rather than meets resistance. Using data we gather during our social engineering tests and password file analysis, we can help facilitate smoother remediation and take you a long way toward building the necessary security habits and disciplines in advance of compliance.