

# Risk Analysis

## Who needs a Risk Analysis?

If you are a covered entity according to the HIPAA Security Standards, you are required by the first subsection of the Administrative Safeguards (S164.308.ii.a) to conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information. You should complete this immediately.

## Why infotex?

We have been conducting technical and administrative security audits since 2000, and our team members have been involved with information security long before then. We offer an analysis process that provides a uniformity that is absent from most technology services. Our team of CISSPs, CISAs, CPAs, Project Managers and Trainers conduct a technical analysis as well as a thorough review of your people, policies, and procedures.

## What makes our Process unique:

Our Risk Analysis 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 any identified vulnerabilities, allowing you to establish acceptable risk.

## Project Management is the Key:

The Risk Analysis is at the top of the HIPAA Compliance Matrix for a reason: 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. 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. Critical path analysis, resource planning, budgeting, and status benchmarks are key tools provided by our methodology.



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

## What is an adequate Risk Analysis?

We believe in a three-pronged approach to risk analysis covering administrative, physical, and technical issues. Our analysis starts with the following assessments:

- Policy/Procedure Review against the HIPAA Security Ruling Compliance Matrix.
- Perimeter testing which 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.

## That’s the Beginning, Not the End!

Our risk analysis is merely a means to an end, and the starting point for your Security Management Process. Our team helps you manage that entire process. Once we have identified, documented, and confirmed the vulnerabilities, we then analyze them from the perspective of threat-level, risk-level, and resources required for remediation. Unlike many assessors who provide a 200 page report full of technical details, we produce an executive summary report that addresses management issues such as overall system condition, budget issues, critical path remediation strategy, and, of course, the vulnerability matrix.

Our matrix includes an index developed with the help of Purdue University’s CERIAS. 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

Though this requirement is not due until the compliance deadline, we recommend that awareness training be one of your first milestones. When all persons associated with your hospital or clinic understands information security, your compliance path gains momentum rather than meets resistance. Not only will this approach facilitate smoother deployment, it will also take you a long way towards building the necessary infosec habits and disciplines in advance of compliance, protecting you from an embarrassing incident on the way to compliance.