



IT Risk Assessment

Using a proven method -- OCTAVE

WHAT IS A RISK ASSESSMENT?

Information security is the process of determining what assets need protection and why, how long they should be protected, what threats are in the environment and lastly how to mitigate those threats.

HOW MUCH SECURITY?

Forrester research has reported that 40% of IT security dollars are spent protecting wrong assets or spent on the wrong risks.

Using a proven IT risk assessment methodology will insure that you are securing the critical assets against real threats balanced against business risks.

WHEN IS RISK ASSESMENT DONE?

It depends on the environment but for the average corporation a full risk assessment is typically done once a year.

WHO NEEDS RISK ASSESSMENT?

The short answer is any company in a competitive environment that has assets that if compromised would materially affect their ongoing business position.

Any business that maintains customer information, deals with personal data, relies on systems (human or computer) to process information.

WHY USE OCTAVE?

The OCTAVE methodology for IT risk assessment is a proven methodology created by the Software Engineering Institute.

OCTAVE is used by government and private enterprises across the US for risk analysis. Using a proven methodology speeds the risk analysis process, ensures completeness, and provides the due diligence necessary in a corporate environment.



BENEFITS AND VALUE ADD

AegisSecurityWorks provides you with a staff of individuals that not only understand information security and OCTAVE but we have extensive experience in software architecture and design, deep understanding of business analysis in a number of domains – Healthcare, retail, financial services to name a few. We also come with a software product **ASW-RiskAnalyzer** that bootstraps and documents the entire process. For you this translates into:

- More complete risk analysis.
- Faster and less expensive process.
- System that will save your risk analysis in a secure location.
- Protecting the right assets against the right threats.
- Create a mitigation strategy that takes into account your individual business risks.

HOW LONG WILL IT TAKE?



The analysis time varies with the complexity of the organization but as a general rule you can plan for 30 to 90 days.

ARE MY STAFF MEMBERS NEEDED?

Yes they are. Typically one to two people are needed 75-80% of the time throughout the analysis and access to subject matter experts is required and the time requirement varies.

HOW MUCH WILL IT COST?

The cost will vary with the size and complexity of the engagement. However, as an estimate of 60 man days at cost of \$75,000 USD. This includes the use of ASW-RiskAnalyzer software (the software can be purchased separately); engagement leaders from **AegisSecurityWorks** will facilitate and manage the risk analysis process.

