



Risk Analysis

OUR FOCUS: DEFINING AND MITIGATING RISK

IAC SecureTech's Risk Analysis is unique in the industry because it forms part of an evolving solutions set for each client's ongoing business processes, as opposed to a profit center designed to point to a pre-determined solution. A risk analysis, tailored to each company's individual risk factors means more useable results.

COST JUSTIFICATION

Additional security almost always involves additional expense. As this does not directly generate income, it should always be justified in financial terms. The IAC SecureTech Risk Analysis process identifies threats and generates security recommendations in business terms.

IAC SECURETECH METHODOLOGY

1. Enumerate informational resources (any asset through which information flows: T1's, routers, switches, servers, etc.).
2. Define interaction between your environment and those outside it.
3. Identify who has control over which resources.
4. Assign priority after enumerating what types of information are:
 - a. Available to the public.
 - b. Available to all in company.
 - c. Available to company, but restricted to certain employees.
5. Identify specific and potential vulnerabilities.
6. Identify controls already in place.
7. Determine which resources require which controls:
 - a. Preventive.
 - b. Detective.
 - c. Corrective.
8. Identify unmitigated residual risk.
9. Recommend levels and types of controls.

PRINCIPLE BENEFITS OF OUR RISK ANALYSIS

- Identification of exposed resources.
- Focus budget dollars and implementation time on highest risk priorities.
- Identification and quantification of risk is an exhaustive exercise that changes with a company's IT environment. However, once completed thoroughly, it is readily tailored to frequent repetition.

Our competitors separate risk analysis from their managed service – we **INCLUDE** Risk Analysis in our Integrated Security Management Service because security is an ongoing process, not an event.

GENERAL BENEFITS OF OUR RISK ANALYSIS

TARGETING OF SECURITY

Security should be directly targeted to potential impacts, threats, and existing vulnerabilities. Failure to achieve this could result in excessive or unnecessary expenditure. Risk Analysis promotes far better targeting and facilitates related decisions. The application of risk analysis across multiple business units enables decision-makers to quickly establish the areas of greatest vulnerability to the enterprise as a whole.

CONSISTENCY

Consistent risk analysis by IAC SecureTech brings a consistent and objective approach to all security reviews, not only across different applications, but different types of business systems. Our risk analysis embraces systems not under the direct control of IT management: paper based systems, PC Systems, or systems utilizing other office equipment.

WELL DEFINED BUSINESS UNIT RELATIONSHIPS

Security is an issue that should be addressed at both executive management and IT staff levels. Business management is responsible for decisions relating to the security risk/level that the enterprise is willing to accept, (which involves consideration of potential business impact). IT management is responsible for decisions relating to specific controls and application.

IAC SecureTech's risk analysis addresses the appropriate policy recommendations to the relevant business units. This approach enhances enterprise-wide understanding of information security, while also helping to further align IT and the business.

