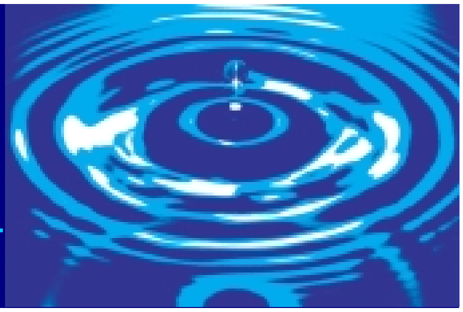
Gould Professional Services, Inc.

Security Planning & Design Services



Security Policy and Risk Assessment

A robust security policy provides documentation of business needs expressed as technological and operational requirements. It is the reference foundation that articulates each organization's unique requirements in a manner that can be directly designed, implemented, and verified. It defines the technical measures that mitigate risk, sets expectations for administrative, user, and employee behavior, and it is a legal document that provides a foundation for the organization to act in a manner that minimizes liability.

Security policy is derived from an assessment of risk. Risk is identified using both a quantitative and a qualitative process that permits a thorough understanding of exposure. Once exposures are identified and understood, it becomes possible to identify industry best practice in activities, technologies and processes to mitigate that risk. The cost of risk mitigation can then be balanced against risk exposure and the potential cost of losses. Having these elements identified and documented permits the calculation of a *Return On Investment,* or ROI for risk mitigation. Operational excellence in risk management and asset protection is the optimum mixture of risk acceptance and risk mitigation through technical and operational processes and capabilities, and is achieved in this manner.

The construction of a security policy document is an important factor in the success of its application. It is well understood that the behavior expectation of all people covered by the plan is set, and the expectations for consequences of deviation from the policy are set. Operational excellence is achieved when technical risk mitigation is thoroughly specified in a technology-independent manner. Decoupling the mitigation elements of policy from the technologies deployed enables the organization to evolve its technical implementation of security while maintaining the linkage to organizational risk. For example, rather than specifying a "firewall" rule requirement, "perimeter security" rules are specified and allowed protocols are addressed, together with an exception approval process to prudently allow for unusual business needs.

Policy enforcement is critical, and in large organizations it may be prudent to develop an enforcement policy that provides management guidance and sets enforcement expectations. Usually such an enforcement policy is part of a manager's guide, and is sometimes private to the management team of the company.

Finally deployment of the policy, ensuring user awareness, and validating operational risk mitigation measures complete the effort. Comprehensive coverage from beginning to end is available, customized to your needs.

Security Policy and Risk Assessment Service Components

Service Component	Inputs	Deliverables
Risk Assessment	Asset identification & valuation	Risk Assessment Document
Behavioral Policy	HR Policies, Security Implementation Plan	Behavioral Policy Elements
Technical Mitigation Policy	Risk Assessment, Security Implementation	Technical Policy Elements
Policy Deployment Audit	Approved Policy, User Interviews, Technology Implementation Assessment	Gaps Analysis and Recommendations
User Policy Training	Approved Policy	Enabled and Empowered Organization

No outsider can make these decisions for you. Rather, by quantifying risk and providing knowledge of how these risks can be mitigated as well as sound cost estimation, you are able to make the decisions that are best for your business. Once the decision processes are complete, the rationale is captured in a Security Policy Analysis, while the specific resulting requirements are captured in a Security Policy document. This unique combination of documentation enables you to readily revisit your requirements as business needs change.