Identify and measure information security risks in your organization.

The Challenge
Today, risks and threats to your proprietary information and IT infrastructure come from everywhere, both inside and outside your organization. It is absolutely critical to identify and understand these threats in order to be able to properly act upon them and reduce your overall risk levels. Achieving this understanding can be difficult due to human and capital resource challenges.

Enter Presidio Cyber Security – your source for expert guidance in the world of risk. Presidio's vulnerability and risk assessment can help you:

- Benchmark your security posture
- Understand vulnerabilities in your environment
- Reduce security risks and liability
- Protect intellectual property and company data

How do we do this?

Risk Analysis
Presidio uses the Risk Assessment portion of the International Organization for Standardization (ISO) information security standard ISO/IEC 27005:2011 as an operating framework for vulnerability and risk assessment engagements. Identified threats are analyzed in light of the value of the asset(s) in question, pervasiveness, effectiveness, existing controls, likelihood of exploitation, and potential impact to the organization if the threat is acted upon. This risk analysis, using an internal risk scoring methodology based on NIST 800-30, results in a risk score that describes the actual risk being incurred due to the existence of the threat or vulnerability and produces comparable and reproducible results in accordance with ISO 27001.

Threat Identification
Threats are identified using a variety of methods, including, but not limited to:

- Gathering of publicly-available information
- Review of existing policies, procedures, frameworks, and processes
- Interviews with various personnel
- Automated and manual technical testing of technology infrastructure
- Review of technology infrastructure architecture and configuration

The Steps to a Secure Organization
- Define a Strategy
- Establish Policies
- Implement System
- Create Awareness
- Monitor Results
- Enforce Compliance
COMPREHENSIVE PHASE-BASED APPROACH

The Presidio vulnerability/risk assessment offering includes assessment of all of the following areas of your organization:

- **Governance** – Assessment of frameworks, policies, procedures, and processes related to information security.
- **Regulatory Requirements** – High-level assessment of compliance with an identified regulatory standard.
- **External Systems** – Vulnerability scanning and validation against Internet-accessible IP addresses.
- **Internal Systems** – Vulnerability scanning and validation against internal IP address ranges and configuration review of all internal systems.
- **Wireless Infrastructure** – Physical assessment of wireless network coverage and security from an on-site perspective.
- **Telephony** – War-dialing tests against organization-controlled phone numbers.
- **Web Applications** – In-depth assessment of Web application security (excluding code review).
- **Penetration Testing** – Activities designed to emulate an actual attack and attempt to access and obtain organizational data.
- **Physical Security** – On-site assessment of the physical security attributes of in-scope locations.
- **Social Engineering** – Customized social engineering attacks testing the effectiveness of existing employee information security awareness and training.
- **Malware** – Analysis of Internet traffic to determine if any internal hosts have been compromised.

In addition, inexpensive follow-up assessment after a period of time validates identified risks that have been directly remediated.

**The Result?**
A clear and comprehensive picture of current risk levels and clear direction as to how best to act upon those risks. Contact Presidio today to start getting the answers you need.

**We are not just trusted partners, we enable new thinking.**