TOP 10 Reasons You Need a Risk Assessment

1 Control Security Spend

Focusing on actual risk, not the latest hot security product, focuses spending on greatest threats.

2 Build a Foundation

Satisfy compliance requirements for an annual risk assessment while arming yourself with information to build your risk management program.

3 Develop a Funding Plan to Reduce Risk

Use information to develop, propose, and justify a spending plan, including added staff and/or other resources.

4 Define What Needs Protection

Determine what your "high value target data" is and how best to protect it.

5 Reduce Time & Resource Usage for Compliance

Auditors typically require your organization to provide artifacts. An assessment produces a number of deliverables which you can use, eliminating the need to reproduce.

6 Integrate Security into IT Projects

Produce a concrete measure of your ability to support new projects securely instead of needing to retro-fit later.

7 Dimenish Mergers & Acquisitions Risk

Mergers and acquisitions produce added risk. Understand what that risk is and how to handle it.

8 Support a Cloud Strategy

Moving infrastructure, applications, and endpoints to the Cloud can save you money. It can also bring added risk. Determine and document risk associated with Cloud Service Providers and moving the environment.

9 Sustain a Network Change

Change equals risk. Understand the changes and impacts a significant network change would bring to your security posture and shield the transition accordingly.

10 Become More Secure

A risk profile helps identify vulnerabilities, capitalize areas of strength, and develop an incident response plan for unknowns.

people connecting people
INTERNETWORK ENGINEERING
since 1996

Knowledge is power. Understanding your risk profile can only come through an I2E Risk Assessment. Contact IE today!