

protect

your business and assets through complete vulnerability analysis

Revealing security weaknesses before an attacker does

Identifying parts of your business that are vulnerable to exploitation is the crucial first step towards remedial action. Analysis of behavior, processes and technology vulnerability will allow you to implement better controls and strengthen confidence and trust in your business.

Complex modern businesses are absolutely dependent on the security of both their information and physical assets. Operating with confidence requires organizations to understand their weaknesses such that they can make balanced judgements concerning risk appetite and treatment.

The issue

Risks to businesses are not always obvious: in fact, they may be quite subtle. And, these risks could exist anywhere—in people, in processes and/or in technology. Yet these subtle, even seemingly minor risks, can have devastating consequences if the proper controls are not put in place. This is why a thorough vulnerability analysis must be performed.

Our solution

Atos offers an enterprise-wide solution with a comprehensive scope. It covers assessment of four security control domains:

- ▶ Physical security
- ▶ IT security
- ▶ Social engineering (people)
- ▶ Process security.

We use a range of analysis tools, security expertise and customized techniques to probe and test each domain. Specialized software tools are used for technical and IT security penetration testing. The output is a report and accompanying presentation, both of which articulate the business risks resulting from the vulnerabilities found. Findings are reported in this context and include recommendations for remedial action.

From vulnerability to strength

The benefits

Our vulnerability analysis service is complementary to the capability that already exists within your organization. It is designed to detect and report potential areas of risk that, suitably addressed, will protect your brand and reputation, support compliance assertions and minimize IP leaks.

Our approach

First of all, we jointly agree the scope of the analysis. We then meet with key members of the technology and business team who have responsibility for operational risk and security and reporting. A schedule is agreed followed by a security testing exercise. Our security testing will try to compromise security, without disrupting normal business operations.

For the technical analysis the Atos team use the same tools that a genuine attacker would use, such as NMAP and Nessus for penetration testing, but we also have the resources to produce customized scripts based on Atos' own IPR, and to utilize a range of commercial tools - AppScan, Retina etc. From their analysis the team produces an issues log. We then investigate each issue in greater depth.

The issues are documented, analyzed in the context of technical and business risk, and written up with recommendations for their mitigation. These are then presented to the stakeholder group.

For us it's all about trust. Our solutions focus on developing trust by managing business risk across the enterprise. In so doing we deliver solutions that transform risk into value.

Why choose Atos?

We help advance your security through a three-stage cycle: Risk and Control Profiling followed by Control Transformation and Business Control Management. Our unique transformational approach is based on integrating the perspectives of people, processes and technology change. We emphasize changing individual behavior as much as we do technology, governance and process.

Atos offers deep domain expertise in vertical markets, bringing to bear an understanding of industry-specific business processes and operating models. Our senior Security and Information Risk Consultants are constantly apprised of best practice through participation in national forums and recognized security organizations - such as the Institute of Information Security Professionals of which we are a corporate founder member.

For more information, visit: atos.net/security, email: security@atos.net or call: Mark N Jones Global Domain Director of Identity, Security & Risk Management on +44(O)7866 767 959.