

Security Best Practices for Sarbanes-Oxley Act Compliance

overview



Security Best Practices for Sarbanes-Oxley Act Compliance

Made Simple

Safeguarding internal controls and procedures for financial reporting, as well as ensuring the confidentiality, integrity and availability of information, is no longer just a best practice for public organizations. It's a legal requirement. Section 404 of the Sarbanes-Oxley Act mandates that all public organizations demonstrate due diligence in the disclosure of financial information and implement a series of internal controls and procedures to communicate, store and protect that data.

Public organizations are also required under Section 404 to protect these controls from internal and external threats and unauthorized access, including those that could occur through online systems and networks. This level of security is necessary to ensure companies maintain data integrity for employees, customers and shareholders.

The business challenges associated with achieving levels of online security that meet Section 404 of the Sarbanes-Oxley Act are abundant, including:

- Lack of definition of security best practices
- Need for interim security while consolidating ERP systems
- Lack of incremental security budget to meet requirements
- Absence of necessary security expertise
- Inability to easily deploy and manage required technology
- Tight deadline in which to achieve compliance
- Lack of employee education on security best practices

Internet Security Systems is prepared to help.

As a world leader in products and services that protect online assets, Internet Security Systems, Inc. (ISS) has demonstrated continued success helping public organizations quickly and simply achieve security best practices that meet the requirements of the Sarbanes-Oxley Act.

Complete Solutions

from a Single Security Partner

ISS is uniquely capable of delivering a complete Sarbanes-Oxley solution that includes the assessment, planning, technology, deployment assistance, education and ongoing management that is needed to remain compliant. ISS delivers a complete solution through:

- **X-Force® Professional Security Services** - An elite team of security professionals that partner with your organization to assess your current security posture and develop a complete roadmap for meeting security best practices.
- **Technology** - Comprises ISS' award-winning solutions spanning the network, server and desktop environments as well as vulnerability detection applications. ISS' SiteProtector™ central management application unifies configuration, deployment and data correlation for all of these agents.
- **Managed Services** - Provides around-the-clock protection for organizations lacking the time, expertise or appropriate internal resources to secure critical information. This comprehensive suite of services provides cost-effective, scalable security solutions through effective leverage of ISS' technology.
- **X-Force Security Intelligence** - ISS' leading group of over 40 security experts, dedicated to proactive counter-intelligence, research, development and public education against online threats, including those facing public organizations. The X-Force tracks the evolution of threats through its Global Threat Operations Center to make sure public organizations are aware of the latest cyber-risks.

The ISS Approach to Security Best Practices for the Sarbanes-Oxley Act

In order to streamline security and help achieve security best practices for Sarbanes-Oxley Act, ISS has developed a five-step process covering the complete security management lifecycle, including phases for Assessment, Design, Deployment, Management and Education (ADDME™). The ADDME process identifies and analyzes gaps in the current security state compared to requirements for security best practices. It then designs and implements solutions to close those gaps and ensure ongoing conformity.

The following phases are part of the ADDME process:

Phase 1: Assessing the current level of information security

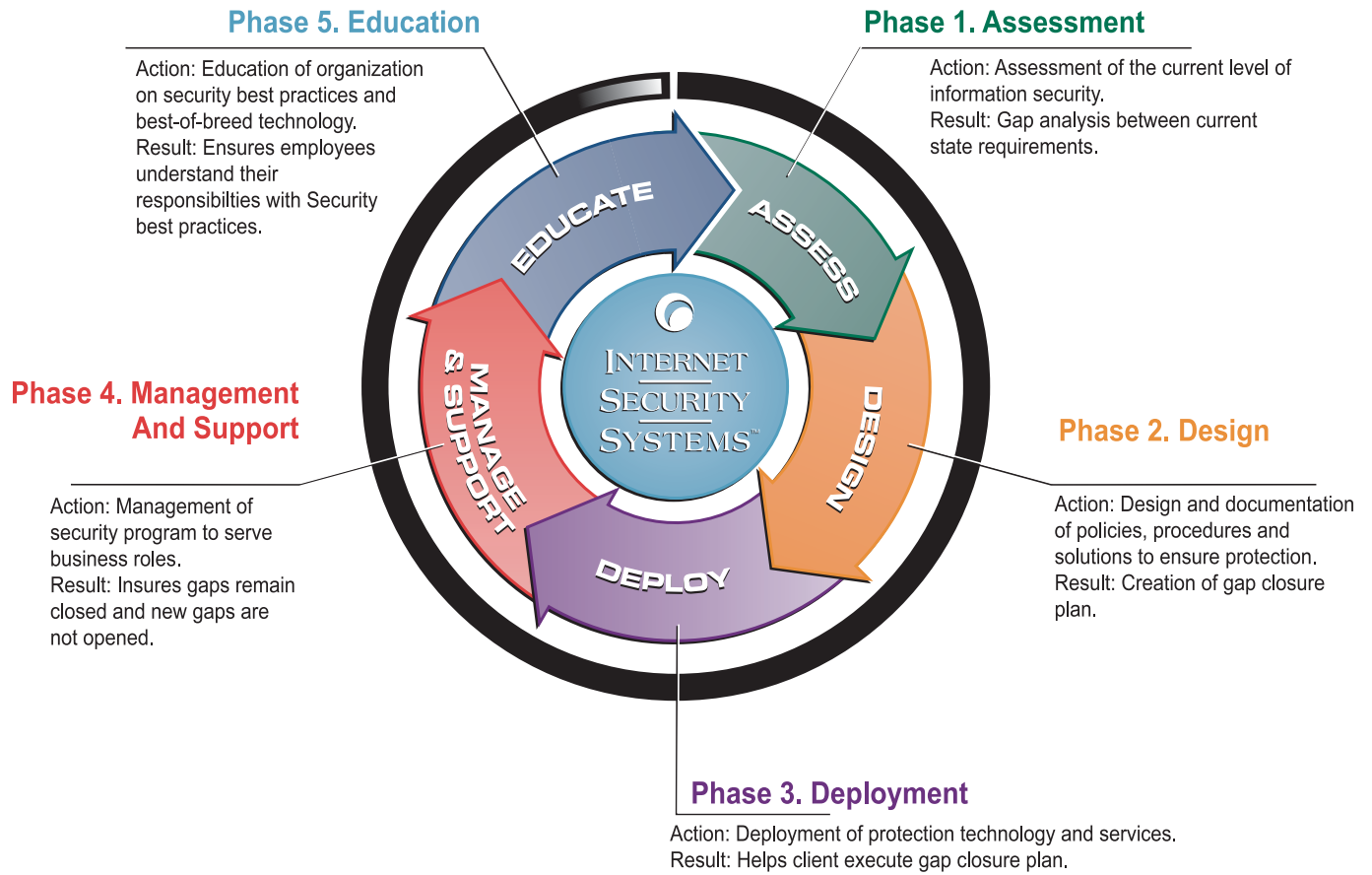
Phase 2: Designing and documenting policies, processes and solutions to ensure protection

Phase 3: Deploying protection technology and services

Phase 4: Managing the security program to serve business goals

Phase 5: Educating the organization on security best practices

The ISS Approach to Sarbanes-Oxley Act Compliance



Get Started Today!

Internet Security Systems offers organizations a single source for guidance, expertise and technology that addresses security best practices for meeting Sarbanes-Oxley requirements. By partnering with ISS, your organization benefits from the best security intelligence and technology in the world, freeing your resources to focus on core business issues and functions.

For more information about the five-step ADDME process and ISS' Dynamic Threat Protection products and services, please visit www.iss.net/products_services/market_solutions/index.php or contact us at 800-776-2362.



INTERNET SECURITY SYSTEMS®

6303 Barfield Road • Atlanta, GA 30328 • Tel: 404.236.2600 • Fax: 404.236.2626 • www.iss.net

About

Internet Security Systems

Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a pioneer and world leader in software and services that protect corporate and personal information from an ever-changing spectrum of online threats and misuse. Internet Security Systems is headquartered in Atlanta, GA, with additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call 888-901-7477.

Copyright © 2004, Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, Proventia, SiteProtector, System Scanner and Wireless Scanner are trademarks and service marks and Database Scanner, Internet Scanner, X-Force and RealSecure are registered trademarks, of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.