

Winfrasoft VPN-Q 2006

White Paper

Achieving Regulatory Compliance for remote access with VPN-Q 2006

Author: Phillip Nicklos
Technical Reviewers: Steven Hope
Published: December 2006
Applies to: Winfrasoft VPN-Q 2006
Web site: <http://www.winfrasoft.com>
Email: support@winfrasoft.com

Regulatory Compliance

Information System Security managers and corporate governance practitioners have always been charged with the responsibility of developing sound controls and performing effective management of internal controls to ensure the availability, integrity and confidentiality of an organisation's information.

Company's business processes are now more transparent to the outside world due to an ever increasing array of regulatory and legislative acts that industry is required to comply with. The regulatory act with the highest importance, and most discussed, is the Sarbanes-Oxley Act of 2002 (SOX). Although this specific act was created for and applies to U.S. security exchanges listed companies, their divisions, subsidiaries and non-U.S. public companies doing business in the United States, similar legislative and regulatory acts are being introduced world-wide.

Overview of Sarbanes-Oxley

The Sarbanes-Oxley Act of 2002 was passed to ensure that corporate executives are held accountable for internal financial controls. Civil and criminal provisions are included in the act to ensure corporate compliance and accountability. However, as financial systems all reside on an IT infrastructure, no assurances for the availability, integrity and confidentiality of financial data can be given without reliance on the internal controls that govern the IT infrastructure. Key sections of the act are:

- *Section 302 - Corporate Responsibility for Financial Reports*
Requires the principal executive and financial officer/officers to certify that submitted reports are both factual and complete and to the appropriateness and reasonableness of internal financial controls.
- *Section 404 - Management Assessment of Internal Controls*
Details the established internal controls, states the responsible parties and assesses the controls effectiveness. External auditors are required to perform an independent assessment of established controls.

SOX is a regulatory act that ensures that industry implements a collection of management and corporate governance controls. Compliance is a highly subjective term as the legislative framework does not spell out, in granular detail, controls, particularly Information Technology related controls, which companies must implement. However, SOX compliance does require institutions to ensure that controls implemented provide reasonable assurance. This is usually achieved by "defence in depth" risk-based approach to infrastructure security and by the implementation of mitigating controls to all apparent and perceived threats.

The Auditing Standard No. 2 of the Public Company Accounting Oversight Board (PCAOB) details the requirements for Auditing Internal Controls over Financial Reports and is a core component of SOX compliance. This standard states that company executives are responsible for the method in which financial data is collected, stored, processed, accessed and generally manipulated.

In essence, this standard enforces corporate executive accountability for all areas of the management of the financial infrastructure down to the networks and computer systems that are used to access this data, irrespective of the physical location of a system. Should a system have access to this data, the system must be governed by predetermined administrative controls. This creates new challenges for remote access solutions which traditionally do not have any knowledge or control over the connecting device.

Coupled to this, the Auditing Standard No. 2 document establishes a recommended framework for evaluating IT controls, called "Control Objectives for Information Technology" (COBIT). The PCAOB document specifically calls for the auditor to examine IT procedures and controls, and the extent to which information technology is used in each financial reporting process.

How does this affect remote access?

As company's infrastructures extend beyond their physical borders, internal controls become increasingly difficult, if not almost impossible, to implement and enforce. Hence acts like SOX require that reasonable assurances are in place to protect the infrastructure i.e. the internal network. It is a well known fact that traditional VPN's are a propagation vector for worms, viruses and malicious code as they "tunnel" through most existing protection systems such as firewalls and IDS, so it is expected that mitigation techniques should be in place to protect against these known threats. SSL VPN's may provide part of the solution but most companies find that they simply cannot do without the traditional IPsec VPN.

Where does VPN-Q 2006 fit in?

VPN-Q 2006 provides management with a reasonably high assurance level of the security and integrity of a remote client's system. VPN-Q 2006's comprehensive battery of endpoint security checks provide reliable assurance that key software and security controls are in place and active before a remote PC is allowed onto the network. Should a remote user's system fail to pass VPN-Q 2006 security and compliance checks, access to the internal network will be limited or barred until such time the compliance issues



are addressed. In addition, records are kept detailing why access was either granted or denied which may be valuable in later forensic analysis.

The following are common controls that, when implemented with VPN-Q 2006 and Microsoft ISA Server, provide the reasonable assurance levels from which regulatory compliance can be gained:

Compliance Control	VPN-Q 2006 Protection
Authentication and access policies that protect against unauthorized access to stored files containing regulated data (strong password policies, file permissions, file encryption, properly configured firewalls)	Strong authentication including 2 factor. Layer 7 EAL4+ firewall when deployed with Microsoft ISA Server.
Policies and implementation of technologies to protect regulated data when it's transferred across the network (IP Security, wireless security).	IPSec encryption and signing to ensure privacy and integrity.
Account policies that strictly define who has access to and control of regulated data (role based administration, delegation of administrative responsibilities)	Per user/group access to specific locations and protocols with the VPN tunnel.
Audit policies that track who accesses regulated data and keeps logs that provide details regarding when, how and by whom such data was accessed. (Audit and event logs)	Log details of who (user name) accessed what resource and when down to the IP and protocol level.
A data protection plan that protects against viruses, Trojans, worms, spyware and other malicious software.	Check endpoint for valid and up-to-date security protection technologies.
An incident response plan for detecting and responding to security breaches that might compromise regulated data	Real-time alerts of suspicious traffic inside the tunnel. Logs showing why a remote system may not be healthy.
Physical security measures to protect regulated data (locked server rooms, locks on file cabinets where paper copies of regulated information are kept, policies requiring workstations be locked down when left alone, disabling of USB ports, floppy drives and other means of copying regulated data to removable media	Ensure that the endpoint cannot be exploited via the console or through network sharing/split tunneling techniques.

Other non-technical controls that require consideration include:

- A disaster recovery plan that ensures that regulated data won't be lost
- Due diligence in hiring of employees and contractors who will have access to regulated data (reference checks, background investigations, requirement that employees sign a confidentiality agreement)
- Training of employees and contractors who have access to regulated data.

Summary

As daunting as compliance as a concept may seem, it cannot be avoided. It is gradually seeping its way into almost every business in every part of the world through one legal act or another. While the legal jargon may vary, the sentiment is the same.

From a remote access perspective, this means taking more care and responsibility for how systems are accessed, not just by whom. In the 21st century, having strong authentication or 2 factor authentication alone is not considered to be enough in terms of due diligence and defense-in-depth to protect remote access connections. VPN-Q 2006 together with Microsoft ISA Server comprehensively cover the bases of strong authentication, health checking, policy compliance, auditing, logging, access control and acceptance which are all key requirements of new legislation.

How compliant is your PC? Check it online now at <http://www.winfrasoft.com/vpnqdemo.htm>

SOX and PCAOB Reference Literature:

For more information on SOX and PCAOB, please refer to the following links:

Sarbanes-Oxley Act of 2002:

<http://www.sec.gov/about/laws/soa2002.pdf>

PCAOB Auditing Standard No 2:

http://pcaobus.org/Rules_of_the_Board/Documents/Rules_of_the_Board/Auditing_Standard_2.pdf

Email: info@winfrasoft.com
Tel: +44 (0)870 236 8346

Web: www.winfrasoft.com
Fax: +44 (0)870 236 8349

