

Sarbanes-Oxley Act Compliance Report

Designated Official: _____

Time Period: 09:54:52 Thursday, July 07, 2005

What is Sarbanes-Oxley Act all about?

The Sarbanes-Oxley (SOX) Act, also known as the Public Company Accounting Reform and Investor Protection Act, was passed by the US Congress in 2002 as a comprehensive legislation to reform the accounting practices, financial disclosures, and corporate governance of public companies.

Whom does SOX affect?

Enforced by the SEC, SOX applies to all companies that are publicly traded in the United States and regulated by the Security and Exchange Commission (SEC).

How does SOX affect IT and network security?

SOX requires that public companies attest to the integrity of their financial controls (section 404). Since IT underlies the very business of financial recording and reporting, this regulation has major implications for IT security. A lack of control over IT security would imply a lack of control over the organization's financial reports, which violates the Sarbanes-Oxley Act section 404. To comply with section SOX 404, publicly companies are expected to use the IT framework developed by IT Governance Institute, also known as Control Objectives for Information and Related Technology (CobiT) to establish appropriate internal controls. Controls over IT security include authentication, access control, user account management, audit controls, data integrity, and encryption.

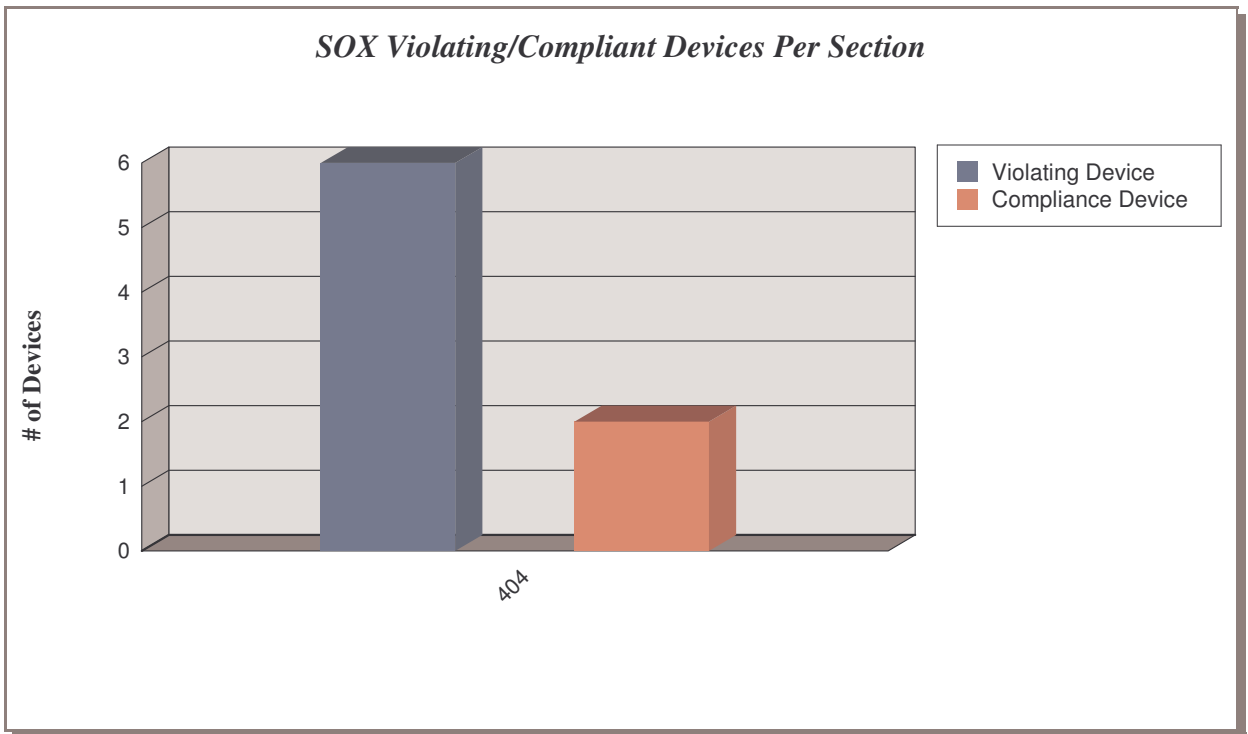
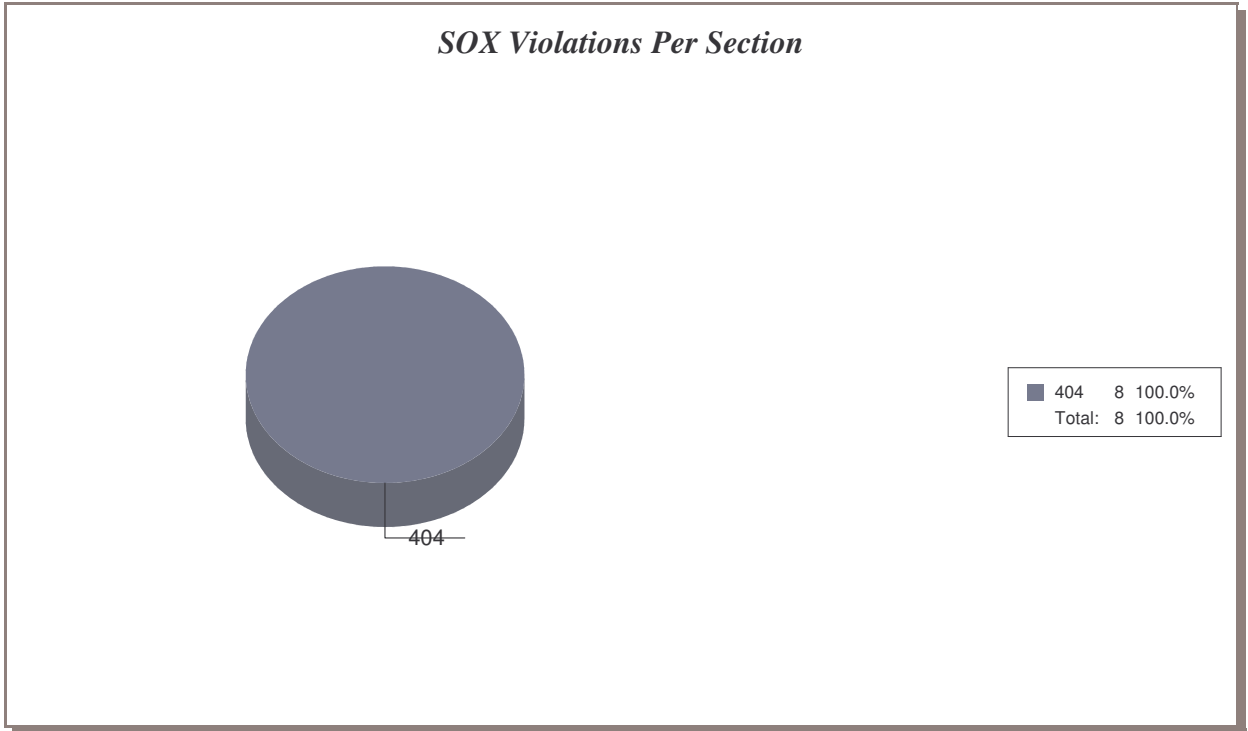
The AirMagnet Sarbanes-Oxley Act compliance report

AirMagnet offers public companies the ability to comply with the stringent IT security mandates of Sarbanes-Oxley. This report covers the major areas the IT security compliance within the context of the Sarbanes-Oxley Act, allowing companies to prove that network security policies are being correctly followed and providing an integral framework to guide network administrators to respond to security threats and incidents in a consistent, compliant, and approved manner.



1/ Policy-Level Compliance Report

This report summarizes your network's compliance on authentication & encryption, and access control, showing you the total number of devices that are in compliance or violation of the network security requirements mandated by SOX.



SOX ITSecurity Performance	Policy Violation	# Violating Devices	# Compliance Devices	Compliance %
404	8	6	2	25.00%

Sarbanes Oxley Act Section 404 Security Requirements			
AirMagnet Alarms	# Violating Devices	# Compliance Devices	Compliance %
404			
WEP IV key reused	1	7	87.50%
AP with encryption disabled	3	5	62.50%
Rogue AP by MAC address (ACL)	3	5	62.50%
Device unprotected by TKIP	1	7	87.50%

Notes:

- 1) By default, your network fails to comply with the Sarbanes Oxley Act (SOX) Section 404 if one of the devices violates a SOX security requirement.
- 2) Channel specific policy violations will not be included in the Device-Specific Compliance Report.

2/ Device-Specific Compliance Report

This report contains detailed information about devices in compliance or violation of the DoD Directive. It checks the devices against each and every provision in the Directive to show what policy provisions are violated or upheld to. It lists all wireless devices deployed on your WLAN. The devices can be sort by MAC address, media type, SSID, or vendor.

Device Information	Policy Provisions	
MAC Address - Type CHANNEL SSID Vendor	Section 404	Compliance %
00:02:6F:20:B3:F7-a Channel: 56 5354a	F	0.00 %
00:02:6F:04:88:6A-b Channel: 1 1d2d70	F	0.00 %
00:0F:66:42:D2:B5-b Channel: 11 kassandra	F	0.00 %
00:02:6F:09:3E:2B-b Channel: 1 1d2d70	F	0.00 %
00:02:6F:20:B3:F8-b Channel: 11 5354g	F	0.00 %
00:02:6F:34:A1:59-b Channel: 6 3054g	F	0.00 %