Fortinet Solutions for Compliance Requirements

Sarbanes Oxley (SOX / SARBOX)

Section / Reference	Technical Control	Requirement	Fortinet Solution
SOX references ISO 17799 for implementation specifics	Firewall	Required	FortiGate
	IDS / IPS	Strongly Recommended	FortiGate
	Centralized Logging	Strongly Recommended	FortiAnalyzer
	Baseline / Vulnerability Assessment	Required	FortiAnalyzer
	Patch Management	24 Hours for Critical Updates	FortiManager, FortiClient
Network Anti-Spyware Network Anti-Virus	Anti-Virus & Spyware Scanning Web, Mail, FTP…	Recommended	FortiGate
Instant Messaging Security	IM Rate Limiting, Logging and/or Prevention	Recommended	FortiGate

Applies to all publicly traded companies. A majority of the regulations apply to auditing, the board of directors, disclosures, and improper trading. Section 404 (below), is interpreted to apply to IT. SOX, as it reads, is highly subjective with few IT specifics. ISO7799, PCI, or HIPAA provide better implementation specifics that you may wish to follow.

IT Requirements Summary:

1. You must have a written security policy.
2. You should baseline your current compliance state and be prepared to show progress towards full compliance. SOX is commonly applied with progressive requirements year over year.
3. Additional sections of SOX require "timely monitoring and response" to issues that may materially affect data used or relied upon to generate public financial

reports. In IT terms – you need to monitor your logs, and respond to threats. SEM tools and IPS are commonly inferred from "timely monitoring."

Gramm-Leach-Bliley Act (GLBA, GLB)

Section / Reference	Technical Control	Requirement	Fortinet Solution
GLBA references ISO 17799 as a guideline	Firewall	Required	FortiGate
	IDS / IPS	Strongly Recommended	FortiGate
Instant Messaging Security	IM Rate Limiting, Logging and/or Prevention	Required (if IM is used/permitted)	FortiGate
	Centralized Logging	Strongly Recommended	FortiAnalyzer
	Baseline / Vulnerability Assessment	Required	FortiAnalyzer
	Patch Management	24 Hours for Critical Updates	FortiManager, FortiClient
Network Anti-Spyware Network Anti-Virus	Anti-Virus & Spyware Scanning Web, Mail, FTP…	Recommended	FortiGate

Applies to the financial services industry (Insurance, Securities, Banking).

With the exception of a few specific acts being made illegal, and fair credit and consumer rights being spelled out, little of the legislation is directly applicable to IT. ISO7799 is referred to as a starting point in many of the legislative summaries and practical implementation guides. PCI or HIPAA provide more tangible implementation specifics, that should, if followed, also provide proper controls for GLBA as well.

IT Requirements Summary:

1. You must have a written security policy.
2. You must establish a baseline – risk assessment – vulnerability scan
3. You must monitor and report on access to any files, folders, or databases that contain consumer financial information.
4. You must notify any consumer if you believe their information has been compromised.

HIPAA – Health Insurance Portability and Accountability Act

Section / Reference	Technical Control	Requirement	Fortinet Solution
High, Medium & Low Systems	Firewall	Required	FortiGate
High & Medium Systems	IDS / IPS	Addressable / Strongly Recommended	FortiGate
16, 18	Centralized Logging	Addressable / Strongly Recommended	FortiAnalyzer
1	Baseline / Vulnerability Assessment	Required	FortiAnalyzer
High & Medium Systems	Patch Management	24 Hours for Critical Updates	FortiManager, FortiClient
17, 19	Encryption	Required (for transmission of patient data)	FortiGate VPN (SSL or IPSEC 3 DES or AES)

The standard and summaries are quite lengthy and verbose in nature, but not difficult to implement, and relatively IT friendly with quite a bit of latitude in methods and implementation specifics.

Applies to organizations colleting, processing or storing medical information, specifically:

Health Care Providers
Health Plans
Health Clearinghouses
Medicare Prescription Drug Card Sponsors

HIPAA - IT Requirements Summary:

HIPAA has an extended set of security requirements and controls with both required and addressable (optional) components. Addressable components of HIPAA not selected must be documented with associated reasoning as to why the specific control was not applied in a given organization. Further classification, and stricter compliance with optional controls are also applied based on system designation as HIGH, MODERATE, or LOW information systems.

A summary of key requirements is listed below:

1. Conduct an initial risk assessment, periodic reviews and reassessments.
2. Written security policy.
3. Designated security person.
4. Written incident handling policy.
5. Backup, Emergency Operations, and Disaster Recovery plan.
6. Reuse and disposal plan for reusable media.
7. Audit controls are required, including unique user identifiers.
8. Termination Policy and Procedures
9. Implement user level processes of least privilege.
10. Log/audit login and logoffs
11. Secure and authenticate before physical access to the facility and sensitive areas is granted.
12. Written usage policies by system type (laptop, desktop, server…).
13. Physical removal tracking and policy of all systems and data (including removable media).
14. Create an “exact copy” backup prior to being moving data or systems.
15. Logout/disconnect inactive sessions
16. Audit access to secure data
17. Encrypt sensitive data
18. Monitor and audit access and alterations to sensitive data
19. Protect data in transmission
20. Multi-Factor authentication and/or non-repudiation

FISMA - Federal Information Security Act (HR 2458-51)

Section / Reference	Technical Control	Requirement	Fortinet Solution
FIPS 199 & 200, DOD 8500.2	Firewall	Required	FortiGate
FIPS 199 & 200, NIST 800-94	IDS / IPS	Strongly Recommended	FortiGate
NIST 800-92	Centralized Logging	Strongly Recommended	FortiAnalyzer
A & B, NIST 800-26	Baseline / Vulnerability Assessment	Required	FortiAnalyzer
NIST 800-40	Patch Management	24 Hours for Critical Updates	FortiManager, FortiClient
NIST 800-77	Encryption (128 bit+)	Required (for transmission of cardholder data)	FortiGate VPN (SSL or IPSEC 3 DES or AES)

FISMA discusses a pyramid of goals based on Availability, Integrity and Confidentiality in order to provide security. Applies to governmental agencies, governmental contractors and telecommunications providers who provide services to anything deemed related to national security (very broad stroke). Also applies to Federal agencies, contractors, and any other company or organization that uses or operates an information system on behalf of a federal agency.

IT Requirements Summary:

There are an extensive series of explicit controls and inter-related publications from NIST and FIPS that specify various controls for Low, Moderate and High Impact systems.

A. Assess Existing State (create a baseline)
B. Create a Risk Assessment Summary, and categorize systems as low, moderate, or high impact relative to security.

1. Check FIPS 199 and determine the class of system (Low, Moderate, High)
2. Review the NIST standards for the type of system (email, DNS, Wireless, etc…)

3. Apply appropriate controls (800-53 appendix D), and amend or create policies (NIST 800-12)

C. Review Internally, and Independently (annually) for compliance.

PCI – Payment Card Industry

Requirement	Technical Control	Requirement	Fortinet Solution
1	Firewall	Required	FortiGate
2	IDS / IPS	Strongly Recommended	FortiGate
4	Encryption (128 bit+)	Required (for transmission of cardholder data)	FortiGate VPN (SSL or IPSEC 3 DES or AES)
5 & 6	Patch Management / Change Control (FW)	24 Hours for Critical Updates	FortiManager, FortiClient
5 & 6	Anti-Virus	Local AV, with Up to date signatures	FortiManager, FortiClient
10	Centralized Logging	Strongly Recommended	FortiAnalyzer
11	Baseline / Vulnerability Assessment	Required	FortiAnalyzer

Applies to merchants and processors of Visa or MasterCard transactions.

Unlike SOX and GLBA, The standard is quite straight forward and IT specific and should be read and reviewed in it's entirety.

IT Requirements Summary:

Taken Directly from the PCI_DSS 1.1 Documentation
1: Install and maintain a firewall configuration to protect cardholder data
2: Do not use vendor-supplied defaults for system passwords and other security
3: Protect stored cardholder data
4: Encrypt transmission of cardholder data across open, public networks
5: Use and regularly update anti-virus software

6: Develop and maintain secure systems and applications
7: Restrict access to cardholder data by business need-to-know
8: Assign a unique ID to each person with computer access
9: Restrict physical access to cardholder data
10: Track and monitor all access to network resources and cardholder data
11: Regularly test security systems and processes
12: Maintain a policy that addresses information security

ISO 17799 / 27001 / BS7799 / NZS 7799 / AS 7799 / IEC 17799

Section / Reference	Technical Control	Requirement	Fortinet Solution
8	Firewall	Required	FortiGate
8	IDS / IPS	Strongly Recommended	FortiGate
11 & 12	Centralized Logging	Strongly Recommended	FortiAnalyzer
6, 7, & 11	Baseline / Vulnerability Assessment	Required	FortiAnalyzer
11 & 12	Patch Management	24 Hours for Critical Updates	FortiManager, FortiClient

Twelve Steps

1. Establish Importance
2. Define the Scope
3. High Level Policy
4. Establish a Security Organization
5. Identify and Classify
6. Identify and Classify Risks
7. Plan for Risk Management
8. Implement Risk Mitigation Strategies
9. Statement of Applicability (gap analysis, exclusions/exceptions)
10. Training and Security Awareness

11. Monitor and Review
12. Maintain and Improve

Focus – Risk Analysis – Threat X Vulnerability – Risk

Common / Non-Specific Requirements Addressed by Fortinet, Inc.

Section / Reference	Technical Control	Requirement	Fortinet Solution
Instant Messaging Security	IM Rate Limiting, Logging and/or Prevention	Recommended	FortiGate
Denial of Service Prevention	DoS / DDoS mitigation	Recommended	FortiGate
IM / P2P Rate Limiting	IM / P2P security Profiles	Recommended	FortiGate
Network Anti-Virus	Anti-Virus Scanning Web, Mail, FTP…	Recommended	FortiGate
Network Anti-Spyware	Anti-Spyware Scanning Web, Mail, FTP…	Recommended	FortiGate
Anti-Spam	Mail profiles – RBL, Black/White, Keywords …	Recommended	FortiGate
Host Based IPS/AV/AS/FW	Client Side Anti-Virus/Spam, Firewall, and Intrusion Prevention	Recommended	FortiClient

Generic Report Output for Compliance (common to nearly all regulations)

1. Logons / Logoffs Successful and Unsuccessful
2. Adding Rights to an Account
3. Adding an account to a group
4. Access to sensitive files (read, or edit)
5. Attacks against systems with sensitive data (Worm, Virus, Buffer Overflow)
6. Breaches of access to any sensitive system

Elements of an Operational Compliance Report

1. Output Should include:
    a. User Event Report
    b. Top Attacker Report
    c. Top Attacks Report
    d. Top Targets
    e. Vulnerability Report
    f. Risk Assessment Report
2. Ideally, to minimize the report length, and improve relevance, you may also:
    a. Identify Critical Assets
        i. Assign Higher Threat Weightings to systems with financial data & critical systems
    b. Segregate Assets that must be audited
        i. Create an Area in SMC for Audited Devices (i.e. accounting area).
        ii. Create IP objects in the audited device area for all critical assets.
    c. Create an Audit Event Attack Method for events that are audit specific (i.e. Windows: 560, 567- File Access, 642 – Account Modification, 628 - Change of Password, 644 - Account Lockout, etc…). And add a report to your compound audit report for by Attack Method to match the custom audit event attack method create.
    d. Annotate each event as cleared with the time it was cleared, who cleared the event, and what the resolution was. Add a report to the compliance compound report for cleared events to include the comments to show timely resolution (not currently required, but somewhat implied).

Summary

Preparing in advance and deploying Fortinet solutions to meet minimum and recommended standards can drastically reduce the length, and cost of compliance audits, and provide the controls, tools, and reports necessary to conform to nearly any compliance regulation.

Basics:

1. A written security policy is a must
2. If you haven't already done an assessment, start as soon as you can.
3. Turn on operating system and application auditing for sensitive data.
4. Create a process to regularly monitor and report on access, failed access, and attacks on sensitive data.
5. Reassess regularly.

A single multi-function integrated Fortinet solution can deliver the security controls needed to assist a well prepared security team in meeting and exceeding any compliance requirement.

Fortinet CSE Team