A Compliance Primer for IT Professionals

David Swift

A Compliance Primer for IT Professionals

GIAC (GSNA) Gold Certification

Author: David Swift
Advisor: Egan Hadsell

Accepted: November 24, 2010

Abstract

Regulations abound and the acronyms are endless. After suffering seemingly endless confusion, I set about in this paper to document the basics of each of the major compliance regulations, to whom they apply, a list of audit frameworks, key IT requirements, and links to best practices and relevant sites. Summary tables are provided up front to condense the bulk of the information into an easily digestible read, with baseline common requirements and reports following. Links to control frameworks, best practices, supporting experts from the legislation, and information on audit types and common compliance reports are provided in appendices. This paper is intended as a compliance starting point for IT professionals, and documents the applicable industry, regulations, controls, audit frameworks, and best practices for major compliance regulations including FISMA, GLBA, HIPAA, ISO, NERC, PCI and SOX.

1. INTRODUCTION

Fed up and frustrated with ambiguous standards, multiple frameworks, and scattered "best practices," I set out to at least glean the basics of compliance. What regulations apply to whom? What do the auditors want to see? And how as an IT security professional can I help reduce my pain, and my company's expenses in successfully completing and passing an audit. I felt it appropriate, and perhaps even beneficial to share that research and hopefully save others time by putting it down in this paper.

As IT professionals we may be required to produce or comply with any number of regulations, auditing frameworks, and best practices. Each is interrelated and can be complex. As a general principal, compliance is about risk: management, identification, elimination, acceptance, and acknowledgement. Risk mitigation efforts should be appropriate to the data and devices being protected. This paper is designed to provide an overview and a basic understanding of the regulations, auditing practices, and industry standards you may be subject to with hyperlinks to relevant sites and related documents. This paper will attempt to identify different possible audits, and a practical reporting framework for IT operational audit compliance. Following charts to help readers identify the sections that apply specifically to their organization, and the specific controls needed, each of the major regulations are summarized. Summary tables are provided up front to condense the bulk of the information into an easily digestible read, with baseline common requirements and reports following. Links to control frameworks (Appendix C - Control Frameworks), best practices (Appendix D – Best Practices), supporting experts from the legislation (Appendix B – Selected Supporting Regulation Exerts), information on audit types (Appendix F - Audit Types), common compliance reports (Appendix A – Common Reports) and terms and definitions (Appendix G – Terms and Definitions) are provided in appendices.

David Swift, dgswift@verizon.net

2. DISCLAIMER

This paper is by no means an exhaustive reference for any given piece of compliance, but rather is designed to help one quickly identify which regulations, frameworks, and best practices are likely to apply, and provide reference links to help one investigate and expand one's knowledge and ability to develop appropriate security and IT audit policies to meet compliance needs. Below follows an attempt to summarize each regulation's sections relative to IT, and provide a suggested superset of controls and reporting data to meet most compliance requirements. A common best practice and next step is to establish a baseline and perform a gap analysis with a professional with knowledge of the specific regulations your organization is subject to.

David Swift, dgswift@verizon.net

3. COMPLIANCE OVERVIEW

Industry	Regulation	Audit Framework	Best Practices
Publicly Traded Company (NYSE, NASDAQ, etc…)	Sarbanes Oxley (SOX, SARBOX)	COSO, SAS70, COBIT	GAAP, ISO, CIS
Bank, Insurance, Securities, Financial, Lenders, Escrow firms	Gramm-Leach-Bliley Act (GLB, GLBA)	COBIT, SAS70 Type II	GAAP, ISO, FDIC, FTC, FFEIC
Hospital, Medical	Health Insurance Portability and Accountability Act (HIPAA)	COBIT, FISCAM	ISO, CMS, NIST
Government, Government Contractors	Federal Information Security Act (FISMA)	FISCAM	FIPS, DISA, NIST, CIS, DCID, DOD, ISO
Credit Card Merchant, Broker, or Clearinghouse	Payment Card Industry (PCI)	COBIT	SANS, ISO, CIS
Electric Generator, Provider or Transmitter	North American Electric Reliability Corporation (NERC), Federal Energy Regulatory Commission (FERC)	ISO 17799, COBIT, ITIL	CIPs, FERC, NIST

Beware: this chart is a generalization. Many companies are subject to multiple regulations, and auditors are not always consistent in choosing the most appropriate framework, nor are best practices agreed upon, or consistently applied.

David Swift, dgswift@verizon.net

4. MAJOR IT REQUIREMENTS BY REGULATION

High Level Requirement	SOX	GLBA	HIPAA	FISMA	NERC	ISO17799	PCI	FIPS200
Written Security & Acceptable Use Policy	•	•	•	•	•	•	•	AC
Audit and Log Security Events	•	•	•	•	•	•	•	AU
Timely Monitoring and Review	•	A	•	•	•	•	•	CM /CA
Risk Assessments (Initial and/or Reoccurring)		•	•	•	•	•	•	CA
Management Sponsorship, Review and Attestation of Security Policies	•	•		•	•	•	•	CA
Separation of Duties (Admin/Security Officer/Auditor)		A	•	•	•	•		
Physical Access Controls (Logs, Barriers, UPS, Cameras…)		A	•	•	•	•	•	AC/ PE
Access and Privilege Management (Individual Accounts, Complex Passwords, Least Privilege, 90 Day change, Min Password...)		A	•	•	•	•	•	AC/ IA
Security/Compliance Awareness Training		I	•	•	•	•	•	AT
Backup/Removable Media Policy (Wipe, Disposal, Encryption, Prevention)		•	•	•	•	•	•	MP
Change Control/Management		A		•	•	•	•	CM
Incident Response / Incident Handling Procedures		A		•	•	•	•	IR
Synchronize System Time (NTP)		A		•	•	•	•	SC/ AU
Policies must be reviewed following significant changes		•		•	•	•	•	CA
Asset Inventory/Classification (High/Medium/Low, Workstation, Server)		A	•	•	•	•		FIP S 199
Incident Tracking / Ticketing		A	I	•	•	I	I	IR
Annual/Quarterly Security Assessment or Audit		A		•	•	•	•	RA
Applications will follow Secure Development Life Cycle (SDLC), processes and review		•		•	•	•	•	SA/ SI
Employee Pre-Screening		A	•	•	•	•	•	
Business Continuity Planning/Disaster Recovery Planning		A	•	•	•	•		CP
Encrypt Sensitive Data at Rest		A	A	I			•	SC
Encrypt Sensitive Data in Transit		A	A	•	I	I	•	SC
Centralized Log Management/SIEM		A		I	I	I	•	AU
Firewalls (Perimeter Defenses)		A		I	I	I	•	SI
IDS/IPS (Perimeter Defenses)		A		I	I	I	•	SI
Anti-Virus Software (Unix is often excluded)				•	•	•	•	SI

David Swift, dgswift@verizon.net

High Level Requirement	SOX	GLBA	HIPAA	FISMA	NERC	ISO17799	PCI	FIPS200
Web Application Firewall (WAF) - SDLC may be accepted in lieu		A			•	•	•	
System Hardening / Standard Configuration		A		•	I		•	CM
Vulnerability Management/Patching		A		•	•	•	•	MA/ SI
Vulnerability Scanning/Assessment		A		I	•		•	SI
File Integrity Checking (FIC) SW		A	A	I			•	SI
No Log Gaps/Log Device Monitoring				•	•	•		
Asses Risks Before Allowing Partner/Extranet/3rd Party Access		•	•	•		•	•	SA
Public Key Infrastructure (PKI)		A	A		•	•	•	
Risk Based Approach		•	•		•			
Notification of Breaches*		•	*		•	•	•	
Written Incident Handling/Incident Response Policy		I	•	I	I		•	
Wireless Networks (Settings, Encryption, Scanning for Rogues…)		A		•	•		•	SC
Designated Security Officer/Contact/Roles		•	•			•	•	
Penetration Testing Network/Application		A					•	
Limit and Encrypt Administrative Access		I					•	
Two Factor Authentication for VPN/Remote Access		A					•	
Personal Host Based Firewalls		A					•	
Data Loss Prevention / Data Leakage Monitoring		A	•			•		

• = Required

I = Implied or Inferred, but not explicitly stated

A = As Appropriate to the Organization (GLBA), Addressable (HIPAA)

* Breach Notification is required by multiple state laws (CA, TX, MN), the HITECH amendment to HIPAA added disclosure requirements.

If blank, the legislation has no discernable reference to the given requirement.

David Swift, dgswift@verizon.net

This table is a high level summary of key requirements, with a focus on common elements, not an exhaustive list. Legal language is open to interpretation, and not everyone will come to the same conclusions. It is better to err on the side of caution and extra security controls when it comes to compliance.

The table above focuses on what the laws require, one should also consider what will be most effective, not just requirements. Several public documents are available that focus on a list of the top security controls; consider Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines v2.3, SANS (2009), Recommended Security Controls for Federal Information Systems, NIST 800-53, (2007).

Reference points for Major IT Requirements Summary by Regulation, and specific minimum requirements are available from multiple sources, including *Minimum Security Requirements for Federal Information and Information Systems*, FIPS 200, NIST (2006), which provides a good baseline and classification of minimum controls, Data Security Standard version 1.2.1 PCI (2009), which lists of over 350 specific controls, *ISO 9000:2005 Quality Management Systems* International Standards Organization, (2005), Financial Institutions and Customer Information: Complying with the Safeguards Rule, FTC (2006), *SUBTITLE A--DEPARTMENT OF HEALTH AND HUMAN SERVICES, PART 164--SECURITY AND PRIVACY*, Code of Federal Regulations, 45CFR164, (2009), as related to HIPAA, and *Critical Infrastructure Protections* NERC, (2006-2010).

Secure Development Life Cycle (SDLC), best practices, common vulnerabilities and a list of common attacks on web applications are available at the Open Web Application Security Project (OWASP) web site.

David Swift, dgswift@verizon.net

The Laws (or governing standard):

5. SOX / SARBOX

Sarbanes-Oxley Act of 2002 (H.R. 3763) 107th Congress (2001-2002)

SOX 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.

SOX - Key IT Requirements Summary

- You must have a written security policy.
- 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.
- 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. SIEM tools and Intrusion Detection/Prevention Systems are commonly inferred from "timely monitoring."
- You must log and audit access to financial data and critical files used in the preparation of public financial reports.

See also Major IT Requirements Summary by Regulation.
See also Appendix B- Selected Support Regulation Experts for SOX specific language.

Related Standards and Items

Public Company Accounting Oversight Board (PCAOB)

David Swift, dgswift@verizon.net

Laws / Standards

6. GLBA, GLB - GRAMM-LEACH-BLILEY ACT

The Gramm–Leach–Bliley Act (GLB), also known as the Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999).

GLBA applies to the financial services industry (insurance, securities, banking), and includes credit reporting agencies, ATM operators, appraisers, couriers, and tax preparers. 313.3(k)

- Specifically makes pretexting illegal.
- 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.
- Section 501(b) however does provide the Federal Trade Commission with a mandate to protect non-public information with "administrative, technical, and physical safeguard" specified by the Federal Trade Commission in 16 CFR Part 314 *Standards for Safeguarding Customer Information* (2002)
- The FTC directives specify safeguards that are "appropriate" to the individual organization, allowing entities of different sizes to select controls that are cost effective, and appropriate to the size and means of the organization.
- ISO7799 is referred to as a starting point in many of the legislative summaries and practical implementation guides.

See also Appendix B- Selected Support Regulation Experts for GLBA specific language.

David Swift, dgswift@verizon.net

Related Standards and Items

Standards for Safeguarding Customer Information 16 CFR Part 314, Federal Trade Commission (2002)

Fair Credit Reporting Act (FCRA)

Financial Privacy Rule

Federal Financial Institutions Examination Council (FFIEC)

See also the FFEIC Audit Handbook for details.

Federal Reserve

"responsible for supervising and regulating banking institutions", and "containing systemic risk" *Overview of the Federal Reserve System*, Board of Governors of the Federal Reserve System, (2005)

Federal Deposit Insurance Corporation

Mission: "examining and supervising financial institutions for safety and soundness and consumer protection" *FDIC Mission, Vision, and Values*, FDIC (2009)

Financial Data Protection Act of 2005

David Swift, dgswift@verizon.net

GLBA – Key IT Requirements Summary

1. Organizations must have a written security policy.
2. Organizations must establish a baseline – risk assessment – vulnerability scan
3. Organizations must monitor and report on access to any files, folders, or databases that contain consumer financial information.
4. Organizations must notify any consumer if you believe their information has been compromised.
5. Organizations must designate a security program coordinator.
6. Organizations must establish and employee security awareness and training program.
7. Organizations must establish policies for information processing, transmission, storage and disposal; and must review and revise following material changes.
8. Organizations must have appropriate measures to detect, prevent, and respond, to attacks and intrusions.
9. Organizations will provide a procedure for FTC reviews or audits.
10. Organizations will provide oversight for contracted service provider organizations.

See also Major IT Requirements Summary by Regulation.

David Swift, dgswift@verizon.net

Laws / Standards

7. HIPAA – Health Insurance Portability and Accountability Act

HIPAA applies to healthcare, medical records, insurance, and other medical related business. Organizations explicitly covered by HIPAA include:

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

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. Security controls are labeled as required, or addressable. Addressable controls are not truly optional, but with proper documentation and compensating controls, or justification as to unreasonable burden to implement, can be made optional.

- A summary of key HIPAA requirements and links is available on the Health and Human Services web site.
- The text of the law is online. The Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Regulation requirements are detailed in Code of Federal Regulations, 45CFR164, (2009)
- See also Appendix B- Selected Support Regulation Experts for HIPAA specific language.

Related Standards and Items

NIST 800-66 National Institute of Standards and Technology documentation for HIPAA

PSQIA - Patient Safety and Quality Improvement Act of 2005

HITECH

- Regulations regarding electronic transmission of patient information.

David Swift, dgswift@verizon.net

- Became effective on February 18, 2009

HIPAA – Key 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. Most technical controls will be in section 164.308.

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 (addressable)
18. Monitor and audit access and alterations to sensitive data
19. Protect data in transmission

David Swift, dgswift@verizon.net

See also Major IT Requirements Summary by Regulation.

Laws / Standards

8. FISMA - Federal Information Security Act

Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, *et seq.*), (2002)

FISMA 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. The main body of FISMA is a snoozefest of legalese with little that is actionable in IT terms. Ironically though FISMA legislation has the least IT related detail, it requires the most from IT to comply as specified in the related NIST, DISA and FIPS standards for implementation and compliance.

- FISMA discusses a pyramid of goals based on Availability, Integrity and Confidentiality in order to provide security.
- Consider and review FIPS 200, *Minimum Security Requirements for Federal Information and Information System* (2006)
- 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.

Related Standards and Items

FIPS Federal Information Processing Standards
DISA Defense Information Systems Agency
NIST National Institute of Standards and Technology

See Appendix E - FISMA Related Guidelines and Best Practices for additional links.

David Swift, dgswift@verizon.net

FISMA – Key IT Requirements Summary

1. Assess Existing State (create a baseline)
2. Create a Risk Assessment Summary, and categorize systems as low, moderate, or high impact relative to security.
3. Classify assets per FIPS 199 (Low, Moderate, High)
4. Secure systems per the appropriate NIST standard by system type (email, DNS, Wireless, etc…)
5. Review Internally, and Independently (annually) for compliance.
6. Implement policies and procedures to reduce risk to an acceptable level.
7. Periodically review and test procedures to ensure effectiveness.
8. Designate a security information officer with primary duties as security.
9. Implement a security awareness training program for staff and contractors.

FISMA compliance makes SOX look easy and fun by comparison.

Laws / Standards

9. PCI – Payment Card Industry

PCI is an independent organization that sets standards for credit card processors and merchants.

- Applies to merchants and processors of Visa, Mastercard, American Express, Diners Club International, or JCB (an Asian based credit card), transactions.
- Current Data Security Standard version 1.2.1, PCI (2009)
- PCI specifies different merchant levels from 1-4 (1 being the highest), based on the number of transactions per year, and has increased security requirements at each higher level.
- PCI specifies security standards for "Any system that stores, processes, or transmits cardholder data"

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

David Swift, dgswift@verizon.net

Related Standards and Bodies

CISP – Cardholder Information Security Protection (Visa)

SDP – Site Data Protection Program (Mastercard)

SB1656- Credit Card Data Disclosure - California Assembly Bill 1656, (2008)

Duty to Protect and Safeguard Sensitive Personal Information, The Data Protection Bill, Texas, Sec. 48.102, House Bill No. 3222 (2005)

Breach of Security, Plastic Card Security Act, Minnesota, SF1574 (2007)

David Swift, dgswift@verizon.net

PCI Specifies six security practices areas and 12 Major Requirements, and over 350 sub-requirements.

TABLE 1 – PCI SECURITY PRACTICES AND REQUIREMENTS

Security Practice	Requirement
1) Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
2) Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
3) Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
4) Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
5) Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
6) Maintain an Information Security Policy	12. Maintain a policy that addresses information security

David Swift, dgswift@verizon.net

PCI – Key IT Requirements Summary

1. You must have a written security policy. It must be communicated to new employees, and have management sponsorship, as well as designating contact information for hosts and emergencies.
2. Annual assessment are required.
3. Quarterly vulnerability scans (annual for level 4 merchants), are required (internal and external).
4. Do not store un-necessary cardholder information.
5. Do not store authentication information (CVV2, PIN) .
6. Encrypt and obscure card information.
7. Systems must be "hardened" to industry standards (SANS, NIST, or CIS)
   a) Patch operating systems and software
   b) Disable unnecessary services.
   c) Change default and vendor passwords and accounts.
8. Firewalls are required, and there are specific policies required for DMZ to Internal, and Internal to External traffic, with both ingress and egress filters.
9. Wireless networks must use their highest possible encryption standard (WPA/WPA2, WEP has been phased out).
10. Protocols should be restricted to HTTP, SSL, SSH, and VPN, except as otherwise noted and justified in a separate written policy.
11. Limit and Encrypt Administrative/Console access.
12. Implement only one function per server (i.e Do not run file service and DNS on the same host).
13. Anti-virus software is required for windows systems (not required on Unix hosts).
14. Applications must follow a Secure Development Life Cycle (SDLC), model with code review.
15. Change control is required.
16. Individual unique accounts, with complex passwords are required.
17. Physical access controls are required (cameras, visitor logs, document shredding…).
18. System auditing (login/logout/system changes….), must be enabled, and backed up to a centralized log server, with 3 months online and one year offline retention.

David Swift, dgswift@verizon.net

19. Penetration testing must be done annually or after significant changes (both network and application layer pen testing).

See also Major IT Requirements Summary by Regulation.

Relevant Sections of the Standard

The entire PCI DSS document pertains to IT controls.

It should be noted that at least 25% of PCI compliance is policy, education and standards based, and not implemented in technical controls, but rather in documentation, and by following standard procedures.

David Swift, dgswift@verizon.net

10. NERC - North American Electric Reliability Corporation

NERC applies to companies that generate, provide, or transmit energy.

- NERC is subject to Federal Energy Regulatory Commission (FERC) mandates and control. NRC (Nuclear Regulatory Commission), is a related commission for nuclear power.
- The primary focus of NERC is on SCADA, which stands for *supervisory control and data acquisition* devices and networks.
- The majority of IT related policies will be found in the Critical Infrastructure Protection Standards (CIP) standards.
- Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets and outlines the key controls relative to IT.
- A key unique issue addressed in NERC is the requirement to monitor log devices with no gap exceeding 7 days. This can be a critical audit finding with serious repercussions.
- Annual reviews of assets, policies, and procedures are mandated.

NERC – Key IT Requirements Summary

Electronic Security (CIP-002, 003, 005, 007, 009)

Under these standards, utilities must:

- Maintain an inventory of all electronics that either are part of the critical assets list or are necessary to the operation of critical assets.
- Protect access to these critical cyber-assets on a need-to-know basis.
- Create an electronic security perimeter that prevents unauthorized users from accessing any critical cyber-asset, whether they are outside or inside the corporate network.
- Ensure that all electronic cyber-assets are secure via user account management, equipment, password management, and secure networking policies.
  - Implement and test a critical cyber-asset recovery plan.

David Swift, dgswift@verizon.net

Physical Security (CIP-006)

Utilities must ensure the physical security of all critical cyber-assets by:

- Ensuring that there is a physical security perimeter around all critical cyber-assets.
- All physical access points to critical cyberassets must be identified and controlled.
- An access log must be maintained for all critical cyber-assets, via keycards, video or manual log.

Personnel Security (CIP-004)

- Each person who accesses critical cyberassets, including the utility's personnel, contract workers and vendors, must be investigated to assess the risk that he or she poses to security.

Training and Awareness (CIP-004)

- Everyone who has access to critical cyberassets, including utility personnel, contract workers and vendors, must be trained in cyber-security.

Audits and Documentation (All CIP standards)

- All CIP standards make it mandatory to document and review all procedures and policies every year. NERC will audit compliance on all the standards on a schedule provided by the organization.

Recovery Plans (CIP-009)

The CIP standards make a recovery plan mandatory. The plan must include:

- Backup strategies
- Data restoration strategies
- Spare parts and equipment.

David Swift, dgswift@verizon.net

11. ISO 27002 / 17799 / BS7799 / NZS 7799 / AS 7799 / IEC 17799

Originally known, and commonly known as ISO 17799, the revised current version is ISO 27002. ISO standards are applied to multinational companies. British Standards (BS), Australian Standards (AS), and New Zealand Standards (NZS), and others were incorporated into a common international framework.

- Available for purchase at ISO.org
- Originally written by the British Standards Institute (BSI).
- ISO 17999 has two primary sections:
  - Code of Practice – guidelines for security management
  - Specification – Audit Controls
- Registering certifies a company for 3 years (requires annual external review).

ISO 27002 – Key IT Requirements Summary

Twelve Steps:

1. Establish Importance
2. Define the Scope
3. Write High Level Policies
4. Establish a Security Organization
5. Identify and Classify Assets and Data
6. Identify and Classify Risks
7. Plan for Risk Management
8. Implement Risk Mitigation Strategies
9. Statement of Applicability (gap analysis, exclusions/exceptions)
10. Implement a Training and Security Awareness Program
11. Monitor and Review
12. Maintain and Improve

See also Major IT Requirements Summary by Regulation.

David Swift, dgswift@verizon.net

Related Standards and items

Information Security Management System (ISMS)

12. Recommended Baseline Controls

Below is a basic list of IT controls and processes to implement to meet a combined minimum for the compliance regulations covered in this document.

1. Create and Maintain a Written Security and Acceptable Use Policy
   - 1.1. Require new employees to review and sign a statement attesting to their understanding of the company's security policy and acceptable use policy.
   - 1.2. Provide any relevant compliance training to new employees and annually for existing employees.
   - 1.3. Document compliance training for all employees, including annual retraining completion.
   - 1.4. Use banners on all publically/remotely accessible systems to inform and require acceptance of acceptable and authorized use.
   - 1.5. Update the policy when there is any material change
2. Document and Maintain an Incident Handling and Incident Response Policy
   - 2.1. Detail Management Sponsorship
   - 2.2. Detail Incident Responders/Security Staff/Contacts
   - 2.3. Document where to find Incident Handling and Incident Response Procedures
3. Implement and Document a Change Management process for all security devices and policies
4. Limit physical access to protected systems
   - 4.1. Log all guest access
   - 4.2. Implement cost justifiable physical controls
     - 4.2.1. Cameras in sensitive areas, and access doors
     - 4.2.2. Badge readers to physically identify access
     - 4.2.3. Limited ingress/egress points
     - 4.2.4. Uninterruptible Power Supplies for critical systems

David Swift, dgswift@verizon.net

5. Document and maintain a business continuity plan
   5.1. Document any offsite facilities to be used
   5.2. Document an out of band communication plan
   5.3. Document key staff and responsibilities
   5.4. Document business critical processes and restoration plans
6. Document and maintain a secure hiring/secure contracting policy
   6.1. Screen all staff as appropriate to their level of responsibility
   6.2. Require third party providers with access to protected systems to comply with company screening/hiring policies.
7. Develop and maintain a dynamic asset inventory system
   7.1. Document the primary function of each system
   7.2. Document the asset owner, and contact information for each system
   7.3. Document asset criticality for each system (Critical/High/Medium/Low)
   7.4. Document the physical location of each system
8. Define and delineate different roles with different people for major security functions
   8.1. Management/Oversight
   8.2. Audit/Review
   8.3. Administration
   8.4. Security
9. Implement a security incident tracking / ticketing tool to log all security incidents.
   9.1. Note the time the incident was detected
   9.2. Note the time the incident was resoled
   9.3. Provide documentation of any discoveries and remediation efforts
   9.4. Track root causes, and implement prevention methods on similar systems to prevent the same root cause from reoccurring
10. Encrypt sensitive data
    10.1. Encrypt data in transit via best available protocols (SSL, SSH, IPSEC…)
    10.2. Encrypt sensitive data at rest using Whole Disk Encryption on laptops and mobile devices.
    10.3. Prohibit, and prevent use of removable media on systems where viable.
11. Use unique user accounts

David Swift, dgswift@verizon.net

11.1. Set a minimum password length of 8 characters
11.2. Require complex passwords (mix of alpha, numeric, and at least one non-standard)
11.3. Prevent reuse of prior passwords, last 9
11.4. Change passwords every 30 days
11.5. Disable any default system accounts
11.6. Prevent anonymous access to all protected systems

12. Log all system access by user, time, and source
12.1. Monitor, Report, and Review Monthly all Administrator Access
12.2. Monitor, Report, and Review Monthly all Service Account Access
12.3. Monitor, Report, and Review Monthly all User Access for terminated employees, or employees with access to unauthorized systems.
12.4. Limit Administrative access to secure protocols (SSH, SSL, IPSEC…).

13. Centrally log all security events
13.1. Store events online for at least 30 days
13.2. Store events offline for 1 year
13.3. If cost justifiable, implement a SIEM for automated threat detection

14. Follow a Secure Development Life Cycle (SDLC), for all applications.
14.1. Perform a code/application review prior to production
14.2. Test for all OWASP known vulnerabilities prior to production for both custom and off the shelf applications.
14.3. Correct, patch, or provide compensating controls for all vulnerabilities discovered.

15. Encrypt all sensitive data in transit via the best available encryption method
15.1. WPA/WPA2 for Wireless
15.2. 256 Bit AES for VPN, 128 Bit SSL minimum

16. Install firewalls at all perimeters
16.1. Including Wireless, Extranet, and any untrusted network boundary
16.2. Enable local firewalls where feasible, consider at least a minimal blocking policy for inbound access to common server ports (20, 21, 22, 23, 80, 135-139, 443, 445)

David Swift, dgswift@verizon.net

17. Install and maintain up to date Intrusion Detection or Intrusion Prevention Systems (IDS/IPS), at perimeter ingress/egress points, including wireless and extranet connections.
18. Install and maintain up to date anti-virus software on all hosts
19. Install perimeter Mail Scanning for Anti-Virus
20. Implement and keep up to date a centralized patch management system
21. Harden all systems
    - 21.1. Remove unnecessary services.
    - 21.2. Disable any unnecessary ports (local firewall)
    - 21.3. Standardize configuration and system images to match NIST, SANS, or another standard baseline.
22. Scan all hosts (Vulnerability Scanning), quarterly
    - 22.1. Remediate or configure compensating controls for all vulnerabilities discovered.
23. Install file integrity checking (FIC), or White listing software on critical systems to prevent and track unauthorized file replacement or modification
24. Implement a restrictive wireless security plan
    - 24.1. Treat wireless networks as untrusted
      - 24.1.1. Pass traffic through a perimeter firewall
      - 24.1.2. Perform IPS and Anti-Virus network level scanning on transfers to/from wireless devices.
      - 24.1.3. Limit wireless use to non-sensitive data, or require additional VPN connection from wireless devices before allowing access to sensitive data
    - 24.2. Scan for rouge access points where feasible.
25. Implement a Web Application Firewall with form/data entry validation for public facing applications, where feasible.
26. Use Public Keys and a PKI infrastructure for public facing applications and trusted email/file exchange where feasible.
27. Use two factor authentication for remote access to sensitive systems/data
28. Perform penetration testing, both external and internal for critical devices and applications relevant to PCI, GLBA, NRC, or SCADA controls.

David Swift, dgswift@verizon.net

13. COMMON COMPLIANCE REPORTS

A common set of reports are applicable to nearly all compliance requirements, and will need to be run and reviewed regularly with supporting documentation. See "Appendix A – Common Reports" for additional details and "Sample Summary Reports" for examples. Also consider the type of audit to be preformed (see Appendix F – Audit Types), when defining reporting goals.

Key Reports

1. All Logons / Logoffs Successful and Unsuccessful
2. Any Rights Additions or Changes for Accounts or Groups
4. Any Access to sensitive files (read, edit, or delete)
5. Attacks against systems with sensitive data (Worm, Virus, Buffer Overflow)
6. Breaches of access to any sensitive system or Personally Identifiable Information (PII)

Elements of an Operational Compliance Report

Output should include:

User Event Reports
Top Attacker Reports
Top Attacks Reports
Top Targets
A Vulnerability Report
A Risk/Threat Assessment Report

Ideally, to minimize the report length, and improve relevance, you may also:

- Identify Critical Assets
- Assign Higher Threat Weightings to systems with financial data & critical systems
- Segregate Assets that must be audited relative to its compliance applicability
- Assign asset criticality properties as appropriate.

David Swift, dgswift@verizon.net

Annotate any event cleared with the time it was cleared, who cleared the event, and what the resolution was.

14. CONCLUSION

Compliance is fun? Well maybe not, but…at least it's perhaps a bit more understandable, and if you have to, you have a good starting point now.

While you may not be subject to all, or even one of these regulations, it is best to assume at some future date you could be required to be compliant with one or more of them and design any comprehensive security solution to meet the common criteria. Also consider that most public policies include the catch all phrase "best practices" subjecting us to not just those most directly linked regulations, but compliance best practices from every regulation.

Basic takeaways:

A written security policy is a must. If you haven't already done an assessment, start as soon as you can. Follow the hyperlinks and review the laws, frameworks and best practices your organization is subject to. Turn on operating system and application auditing for sensitive data. Create a process to regularly monitor and report on access, failed access, and attacks on sensitive data. Reassess regularly.

Implementing the recommended baseline controls outlined in, Recommended Baseline Controls, and common compliance reports outlined in Common Compliance Reports, will cover a great deal of ground toward any compliance effort.

Being prepared will make getting through it much easier. Even if you're not subject to federal compliance, best practices provided by NIST, SANS and CIS (see Appendix D – Best Practices) can enhance your overall security profile and improve your compliance standing.

David Swift, dgswift@verizon.net

15. REFERENCES

Critical Infrastructure Protections (2006-2010).

Financial Institutions and Customer Information: Complying with the Safeguards Rule, FTC (2006).

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, NIST (2006).

ISO 9000:2005 Quality Management Systems (2005)

Kerr, Orin S, *Computer Records and the Federal Rules of Evidence* retrieved from October 18, 2010 from U.S. Department of Justice.

NERC CIPs and Standard, Retrieved October 18, 2010 from the North American Electric Reliability Corporation.

Payment Card Industry Data Security Standard v1.2.1 (2009), Retrieved October 19, 2010 from the PCI Security Standards Council.

Sarbanes-Oxley Act of 2002 (H.R. 3763) 107th Congress (2001-2002) Retrieved October 18, 2010 from the Library of Congress.

SUBTITLE A- PART 164--SECURITY AND PRIVACY, Department of Health and Human Services (2002).

The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, *et seq.*), Retrieved October 18, 2010, from the National Institute of Standards and Technology.

The Gramm–Leach–Bliley Act (GLB), also known as the Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999), Retrieved October 18, 2010 from the Federal Trade Commission.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) Retrieved October 18, 2010 from the U.S. Department of Health and Human Services.

David Swift, dgswift@verizon.net

16. ACKNOWLEDGEMENTS

Thank you to Accuvant (my employer), for allowing me to share the included content, having developed and/or refined much of it "on the job" at numerous client installations.

Special thanks to Evan Tegethoff of Accuvant's risk and compliance management practice for sharing real world best practices and more documentation than I can absorb. I read until my eyes started to bleed, and tried to summarize an entirely new view of IT and security requirements.

Thanks again to Egan Hadsell @ SANS for editorial advice.

I owe general credit to SANS courses for information and processes that have become part of my standard way of thinking, if not specifically quoted in the paper.

SANS Audit 507, Auditing Networks, Perimeters and Systems, 2006
SANS Security 504, Hacker Techniques, Exploits and Incident Handling, 2009
SANS Security 503, Intrusion Detection In-Depth, 2006

David Swift, dgswift@verizon.net

APPENDIX A – COMMON REPORTS

These reports are produced and reviewed monthly, or on demand as needed.

User Activity Reports

User activity reports should be reviewed/certified as valid by the administrator/manager for each authentication source. Unused accounts should be disabled. Any unexpected account usage (Guest, Root, Administrator, or other vendor default account usage, terminated employees…), should be investigated and explained.

- All Active User Accounts (any valid/successful login by account name in the past 30 days)
- Active User List by Authentication type (Active Directory, RADIUS/TACACS, Local Unix/Windows, SSH)
- VPN Users
- Active Directory Users
- Infrastructure Device Access (Firewalls, Routers, Switches, IDS)
- User Creation, Deletion and Modification
    - A list of all user accounts created, deleted or modified by authentication type, to include the date, time, and User ID that made the change.
- Access by any Default Account
- Access by any terminated employee, expired contractor, or other expired account
- Access by Privileged Accounts (root, administrator…)
    - Include time, date, source IP, and where possible source user name that e became admin or root (su log) or executed a privileged operation on Windows (Reboot, Log Clear, File Deletion).
- Service Account Usage
    - A list of all service accounts grouped by target address
    - This report should be reviewed by the service account user owner and validated monthly.
    - Any unexpected use of a service account, or use on an unexpected address should be investigated and explained.

David Swift, dgswift@verizon.net

Configuration Change Reports

Any configuration changes on monitored devices

Note the Date, Time, and User ID that made the change

Access Reports

- Access to any protected/monitored device by an untrusted network
- VPN Access to Protected Network
- Wireless Access to Protected Network
- Access by a Foreign Network to a Protected Network
- Foreign Country – traffic to/from a foreign country grouped by country
- Any Non-Internal/Company/Intranet Source Address
- Access to a Higher Security Network by a Lower Security Network
- Internet Usage by Protected Device
- Any traffic from a protected device to a network other than the protected and trusted networks.

Incident Tracking

Details should include the total time the ticket was open (Time to Resolution), the root cause if found, and the person who opened and closed the ticket.

- Current Open Ticket List - A list of all incidents not yet closed.
- Closed Ticket Report - A list of all tickets closed in the past X days (from 1-90).
- Time to Resolution by Ticket Type
    - For each ticket type (See Attachment A – Required Correlations), the minimum, maximum, and average time to resolution.

David Swift, dgswift@verizon.net

On Demand Operational Reports

- User Login Tracking
    - All Logins for a User ID for the past 30 days - Group by User Name and Source Address
    - Use: Identify any Hosts a Terminated/Suspicious employee has logged on to for secondary investigation of those hosts.
- Host Login Tracking
    - All logins on a given host for the past 30 days
    - Use: Identify who may have compromised a host that is misbehaving.
- Malware Source Report
    - A list of host addresses for any identified malware or attack – group by malware name or attack name
    - Use: Identify the source IP addresses of any given malware or attack for targeted removal/remediation.
- Malware Occurrence Report
    - A count of any given malware (group by IDS signature/Anti-Virus Signature/Attack Name), over the past 30 days.
    - Use: Defense Tuning – if <100 occurrences of a signature, block, If >100,000 blocking could disrupt the network. Log only mode on new signatures for 30 days, monitor, and block as appropriate.

David Swift, dgswift@verizon.net

Monthly Summary Reports

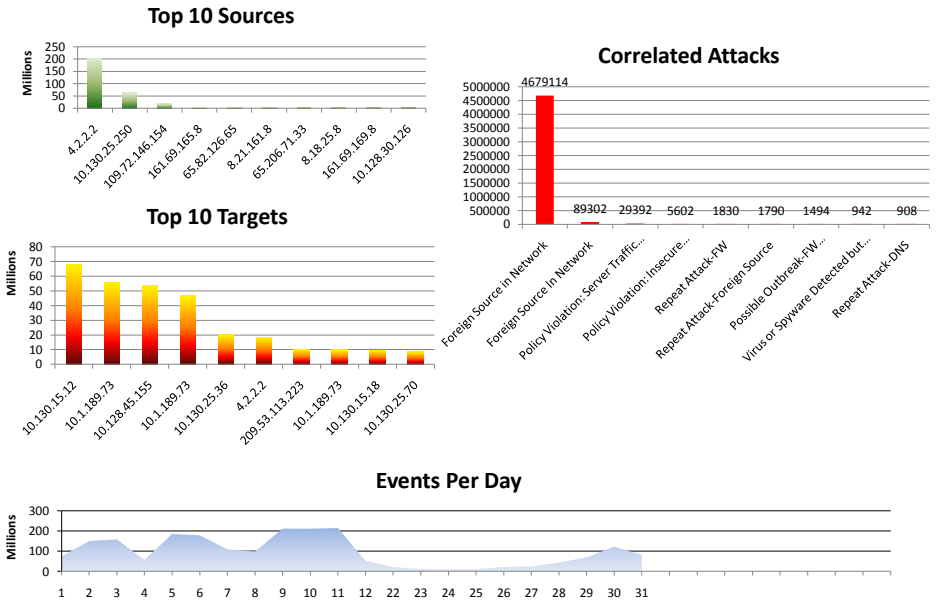
These reports are produced and reviewed monthly.

- Top Sources & Destinations
    - Filter to remove known servers
    - This report should identify unexpected servers and traffic sinks
- Total Correlated Events/Events of Interest
    - Grouped and totaled by Event of Interest/Correlation name
- Total Events / Day / Log Source
- Top 10 Events Per Log Source (Anti-Virus, IDS…)
- Top 10 Failed Logins
    - Grouped by Source IP (Top 10 sources of failed logins)
    - Grouped by Target User Name (Top 10 accounts with failed logins)
- Web Content Filter Summary
- Top 10 Destinations by Domain Name
- Top 10 Blocked Sources by IP Address
- Top 10 Blocked Sources grouped by Network (subnet)
- Foreign Attacker Report
    - Top 10 Source Countries involved in Attacks (FW, IDS, AV, AUTH…)
    - Top 10 Sources IPs of Foreign Attacks
    - Top 10 Destinations of Foreign Attacks

David Swift, dgswift@verizon.net

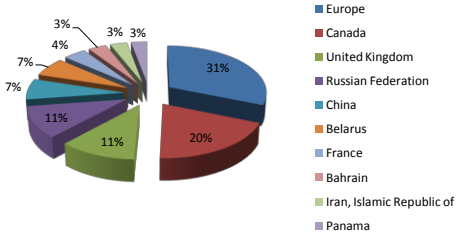
Sample Summary Reports

Monthly Summary Report – SIEM Overview



Monthly Summary Report – Foreign Attackers

Top 10 Source Countries



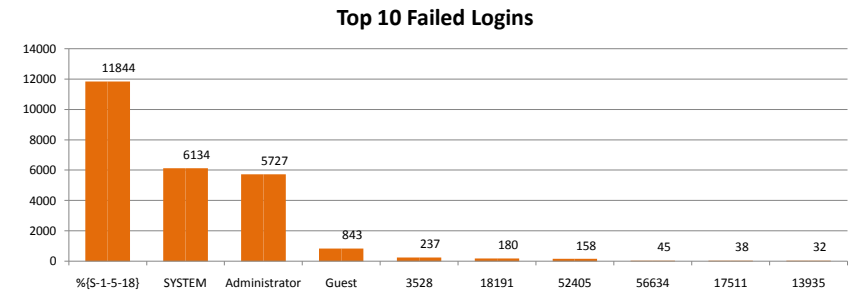
Top 10 Foreign Attackers

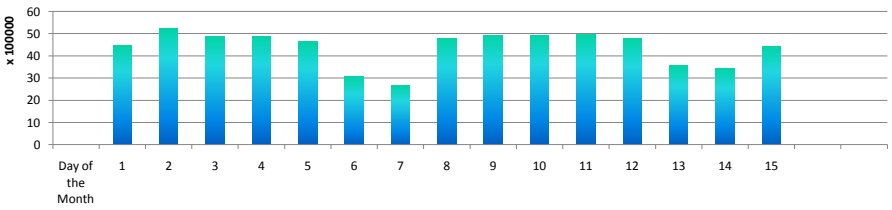
109.72.146.154	Europe	15393914
188.72.213.59	Belarus	2977444
91.212.135.186	Russian Federation	2699576
91.212.135.136	Russian Federation	2249550
91.205.41.235	United Kingdom	1758810
193.104.12.102	Panama	1375574
64.71.246.28	Canada	1056001
91.205.41.164	United Kingdom	1042430
24.153.22.142	Canada	996563
109.72.146.155	Europe	962600

A large number of the attacks, are targeting DNS (port 53), and may have been exploiting previous weaknesses now patched with Windows 2008 upgrades to DNS Servers and Domain Controllers.

David Swift, dgswift@verizon.net

Monthly Summary Report – Authentication





Monthly Summary Report - NIPS

Blocked Attacks

WORM: W32/Netsky@MM Worm 163	399
SMTP: Incorrect MIMEHeader with Executable Attachment Found 94	146
WORM:W32/MyWife.d@MM 48	45
SHELLCODE: Shellcode Detectedfor HP PA-RISCFamily CPUs 23	33
WORM: W32/Zafi@MM Worm 23	29
DCERPC: SRVSVC Buffer Overflow 20	25
NETBIOS-SS: Microsoft Server Service Remote Code Execution Vulnerability 5	4
PCANYWHERE:Host Logon Engine Buffer Overflow 2	3
WORM: W32/Netsky@MM Worm VariantsII 2	3
BACKDOOR: Web Serve CT Backdoor 2	2
SMB: NLTMSSP_AUTHUnauthorized ChangeServiceConfigW Request 1	1
Total:	690

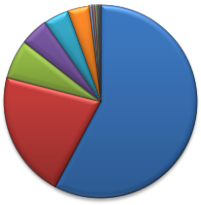
Severity Counts

Blocked	690
High	8,902
Medium	9,148,414
Low	7,017,018
Unclassified	37,092,444
Total:	**53,267,468**

Approximately 700 malicious attacks were blocked in the past 30 days

Network Intrusion Prevention Systems (NIPS)

Top 10 Blocked Attacks



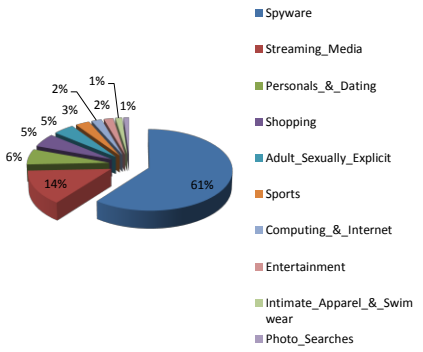
- WORM: W32/Netsky@MM Worm 163
- SMTP: Incorrect MIMEHeader with Executable Attachment Found 94
- WORM:W32/MyWife.d@MM 48
- SHELLCODE: Shellcode Detectedfor HP PA-RISCFamily CPUs 23
- WORM: W32/Zafi@MM Worm 23
- DCERPC: SRVSVC Buffer Overflow 20
- NETBIOS-SS: Microsoft Server Service Remote Code Execution Vulnerability 5
- PCANYWHERE:Host Logon Engine Buffer Overflow 2
- WORM: W32/Netsky@MM Worm VariantsII 2
- BACKDOOR: Web Serve CT Backdoor 2
- SMB: NLTMSSP_AUTHUnauthorized ChangeServiceConfigW Request 1

David Swift, dgswift@verizon.net

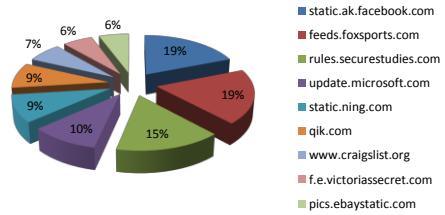
Monthly Summary Report - WCF

Web Content Filtering (WCF)

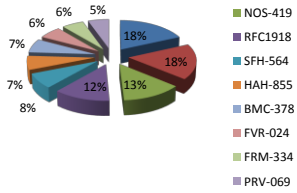
Top Blocked Categories



Top Blocked Destinations



Top Blocked Locations



5

David Swift, dgswift@verizon.net

APPENDIX B – SELECTED SUPPORTING REGULATION EXERTS

SOX

Sarbanes Oxley (SOX) , though widely applicable to any publically traded company, can be a difficult document from which to infer IT requirements. However SOX provides language, which when interpreted in an IT context translates to "we must log events, and respond in a timely fashion. From *Sarbanes-Oxley Act of 2002* (H.R. 3763) 107th Congress (2001-2002) SEC. 103. AUDITING, QUALITY CONTROL, AND INDEPENDENCE STANDARDS AND RULES. (c)(2 "The Board shall respond in a timely fashion to requests from designated professional groups of accountants and advisory groups...."

While the focus of the bill is on auditors, and financial reporting, supporting logs and data to which the board is required to attest to often fall on the heads of IT professionals to provide.

Sarbanes Oxley, also provides a base timeline of one year for event retention. Again, though not technology directed, actors subject to the law are required to provide annual reports, and both annual and one year appear repeatedly in the law. From section 404 "MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS. (a) Rules Required.--The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall--

> (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
>
> (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting."

Sarbanes-Oxley Act of 2002 (H.R. 3763) 107th Congress (2001-2002) SEC. 404.

David Swift, dgswift@verizon.net

David Swift, dgswift@verizon.net

GLBA

Title 5 Requires a Security Policy consisting of three critical phases.

Establish

Asses

Manage

Section 501 of GLBA requires financial institutions to protect non-public information with "administrative, technical, and physical safeguards."

> SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.
> (b) FINANCIAL INSTITUTIONS SAFEGUARDS.—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
> (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999)

The controls required by section 501, are defined by the Federal Trade Commission in 16 CFR Part 314.4 Elements in *Standards for Safeguarding Customer Information* (2002)

Federal Trade Commission in 16 CFR Part 314.4 Elements (b) in *Standards for Safeguarding Customer Information* (2002) ''identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or the compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.''

David Swift, dgswift@verizon.net

Financial Data Protection Act of 2005

"Whenever any consumer reporter that maintains or receives sensitive financial personal information for or on behalf of another party determines, or has reason to believe, that a breach of data security has occurred with respect to such information, the consumer reporter shall:

(A) promptly notify the other party of the breach;

(B) conduct a coordinated investigation with the other party as described in subsection (b); S 2169 IS and

(C) ensure that the appropriate notices are provided as required under subsection"

109th Congress 1st Session, H.R. 3997, *Financial Data Protection Act of 2005*, (2005)

HIPAA

45 CFR § 164.530

(c)(1) Standard: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) Implementation specification: safeguards.

(i) A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure." The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191)

45 CFR § 164.308 – Administrative Safeguards

"Implement policies and procedures to prevent, detect, contain and correct security violations."

David Swift, dgswift@verizon.net

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."
"Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."
"Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3) i)(B) of this section."
"Procedures for guarding against, detecting, and reporting malicious software."
"Procedures for creating, changing, and safeguarding passwords." The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191)

45 CFR § 164.310 – Physical Safeguards
"physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."
"Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."
"Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."
"Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision."
"Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks)."

David Swift, dgswift@verizon.net

"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility."
"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment." The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191)

45 CFR § 164.312 – Technical Safeguards
"the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."
"Assign a unique name and/or number for identifying and tracking user identity."
"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."
"Implement a mechanism to encrypt and decrypt electronic protected health information."
"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."
"Implement electronic protected health information has not been altered or destroyed in an unauthorized manner."
"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191)

FISMA

''§ 3544. Federal agency responsibilities
(a) IN GENERAL.—The head of each agency shall—
(1) be responsible for (A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or

on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;" The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, *et seq.*),

NERC CIPs Critical Infrastructure Protections

North American Electric Reliability Corporation, (2010)

Critical Infrastructure Protection (CIP)	
Number	Title/Summary
CIP-001-1	Sabotage Reporting Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.
CIP-001-1a	Sabotage Reporting Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.
CIP-002-3	Cyber Security - Critical Cyber Asset Identification NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

David Swift, dgswift@verizon.net

	Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.
CIP-003-3	Cyber Security - Security Management Controls Standard CIP-003-3 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3
CIP-004-3	Cyber Security - Personnel & Training Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.
CIP-005-2a	Cyber Security - Electronic Security Perimeter(s) Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.
CIP-005-3	Cyber Security - Electronic Security Perimeter(s) Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

David Swift, dgswift@verizon.net

CIP-006-3c	Cyber Security - Physical Security of Critical Cyber Assets Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.
CIP-007-2a	Cyber Security - Systems Security Management Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.
CIP-007-3	Cyber Security - Systems Security Management Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.
CIP-008-3	Cyber Security - Incident Reporting and Response Planning Standard CIP-008-3 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-23 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.
CIP-009-3	Cyber Security - Recovery Plans for Critical Cyber Assets Standard CIP-009-3 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-3 should be read as part of a group of standards numbered Standards CIP-002-3 through

David Swift, dgswift@verizon.net

	CIP-009-3.

David Swift, dgswift@verizon.net

APPENDIX C - CONTROL FRAMEWORKS

COSO – 5 Internal Control Components – Primary Reference for SOX

1. Control Environment
2. Risk Assessment – maps only to a method in COBIT
3. Control Activities
4. Information & Communication
5. Monitoring

COBIT

COBIT is closely related to both the IT Governance Institute (ITGI) and Information Systems Audit and Control Association® (ISACA®). Certified auditors, and COBIT references are identified and published on the ISACA website (www.isaca.org).

COBIT defines four domains:

1. Planning and Organization
2. Acquisition and Implementation
3. Deliver and Support
4. Monitor and Evaluate

Stated Goals:

Effectiveness, Efficiency, Confidentiality, Integrity,

Availability, Compliance, Reliability

SAS 70

SAS was created by the American Institute of CPAs (AICPA).

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the AICPA. There are two classifications of SAS70 audits – Type I (no verification), and Type II (with test and verification and documentation supporting testing of controls).

David Swift, dgswift@verizon.net

FISCAM

Federal Information System Controls Audit Manual

ITIL Information Technology Infrastructure Library

ISO 9000

International Standards Organization, ISO 9000:2005 Quality Management Systems

David Swift, dgswift@verizon.net

APPENDIX D – BEST PRACTICES

NIST – National Institute of Standards and Technology

NIST 800 series publications document best practices for many IT devices and policies. Even if you're not subject to federal compliance, a NIST has a wealth of good documentation on securing nearly any type of device that can help in meeting any compliance goal. Most of the publications are free and available for electronic download.

ISO/IEC 17799 Code of Practice for Information Security Management

The International Standards Organization maintains a baseline set of common requirements for companies operating outside of the United States.

DOJ - Department of Justice

With respect to log usage for forensics, auditing and compliance, the department of justice standard states with respect to rules of evidence "If a business routinely relies on a record, that record may be used as evidence."
http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm
If you ever intend to prosecute a cyber crime, knowing and complying with DOJ standards of evidence and custody of evidence will significantly improve your chances.

FIPS - Federal Information Processing Standards

FIPS publications document government related IT standards and requirements.
A list of key publications including FIPS 199 and 200.

CIS - Center for Internet Security

CIS provides assorted standards for system hardening and security.

CMS - Centers for Medicare and Medicaid Services

CMS is a clearing house for HIPAA, and other medical related information.

David Swift, dgswift@verizon.net

DISA - Defense Information Systems Agency

DISA provides defense related industry standards, instructions, and guidance.

GAAP – Generally Accepted Accounting Principles

Set by the Financial Accounting Standards Board (FASB), may appear as FASB-#

Related: American Institute of Certified Public Accountants (AICPA)

David Swift, dgswift@verizon.net

APPENDIX E - FISMA RELATED GUIDELINES AND BEST PRACTICES

FIPS 140-1

FIPS 140-2 Security Requirements for Cryptographic Modules

FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems

FIPS 200 – Minimum Security Requirements for Federal Information and Information Systems.

FIPS 201 Personal Identity Verification (PIV)

ISO/IEC 17799 – Code of Practice for Information Security Management

DOD 8500.2 - Information Assurance (IA) Implementation

http://www.dtic.mil/whs/directives/corres/html/85002.htm

DCID 6/3 – Director of Central Intelligence Directive

PROTECTING SENSITIVE COMPARTMENTED INFORMATION WITHIN INFORMATION SYSTEMS http://www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm

NIST 800 Series Publications

NIST 800-12 An Introduction to Computer Security (Procedures and Policies)

NIST 800-16 Security Awareness Training

NIST 800-18 Guide for Developing Security Plans for Federal Information Systems

NIST 800-26 Security Self Assessment Guide

NIST 800-28 Active Content and Mobile Code

NIST 800-30 Risk Management Guide for Information Technology Systems (Risk Mitigation)

NIST 800-32 Public Key Technology

NIST 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems

NIST 800-40 Security patch installation and patch management

NIST 800-41 Guidelines on Firewalls and Firewall Policies

NIST 800-44 Guidelines on Securing Public Web Servers

NIST 800-45 Email Security

David Swift, dgswift@verizon.net

NIST 800-47 Connecting information systems

NIST 800-48 Wireless Networks

NIST 800-50 Security Awareness Training

NIST 800-52 Transport Layer Security (TLS)

NIST 800-53 *Second Draft Special Publication 800-53 Revision 1 Recommended Security Controls for Federal Information Systems* (176 page overview)

NIST 800-53 *VOIP*

NIST 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories

NIST 800-61 Security incident handling and audit record retention (attack detection)

NIST 800-63 Remote electronic authentication

NIST 800-73 Cryptographic verification or biometric verification.

NIST 800-76 Biometric verification

NIST 800-77 IPsec-based virtual private networks

NIST 800-78 Token-based access control

NIST 800-81 Secure DNS

NIST 800-83 Malicious Code Protection

NIST 800-92 Security log management

NIST 800-94 IDS/IPS including Wireless

NIST 800-95 Secure Web Services

NIST 800-97 Wireless Networks

In case you're wondering, yes, there is a NIST 800-1 right through 800-103, along with nearly 200 NIST 500 series standards.

David Swift, dgswift@verizon.net

APPENDIX F - AUDIT TYPES

Before an compliance audit and creation of reports, one must consider the type of auditing to be preformed.

Three types of audits are common:

Compliance / Policy / Management

- An audit of policies, procedures, and confirmation of signatures (written documentation).
- Often for external sources (Government Regulations, Accounting)

Internal / Device / Software

- An audit of software revisions, rules, and device level compliance.
- An audit of compliance with software licensing agreements.
- A listing of hardware devices and software in one's network.
- Very detailed, usually gathered with individual software tools (RAT, Nessus, MBSA…).

Operational Audit

- Are policies and procedures being followed?
- Are backups being performed?
- Is access to sensitive data and locations monitored and recorded?
- Are devices working properly and blocking what they should (penetration testing)?
- Are proper procedures in place and being executed to meet "timely monitoring and response" Service Level Agreements?
- May be used as output for part of a compliance audit.

David Swift, dgswift@verizon.net

APPENDIX G -TERMS AND DEFINITIONS

ISO – Information Security Officer, International Standards Organization

ISSM – Information Systems Security Manager

ISMS – Information Security Management System

CPI - Continuous Process Improvement

PII – Personally Identifiable Information

Threat = Exploit + Vulnerability – Compensating Controls

Compensating controls can include firewalls, and any active preventative security device (IPS, Anti-Virus, HIPS, File Integrity Software (Solidcore, Deepfreeze…) SIEM and passive detection devices, while helpful in identifying threats, are not compensating controls. These type of tools reduce MTD (Mean Time to Detect). A threat does not exist until an exploit exists in the wild that can compromise the vulnerability.

Exposure = Accessible Vulnerability

A vulnerable device that cannot be accessed is not exposed

An exposure exists when a vulnerable device does not have mitigating compensating controls

Threat Detection = Attack + Change in Behavior by Target

Repeat attacks in and of themselves do not constitute threats

A true threat occurs when an attacked asset changes behavior

Repeat Failed Logins followed by Successful Login (possible brute force)

Known Attacker (Black List Source), successfully connects followed by IRC/BOT Control traffic

Malware detected (IDS, AV, HIPS), followed by unusual traffic (port scan, host scan, repeat firewall drops to multiple destinations – common worm symptoms)

David Swift, dgswift@verizon.net