

# The Convergence of Risk Management and Compliance

# Agenda

- Regulations and other government “guidelines”
- Risk Management – the classical approach
- Failings of the classical approach
- 10 minute break
- Changing how we look at compliance
- Security Standards – a “new” way to approach Compliance.
- Risk Management moving forward.
- A few take aways
- Q & A

# Regulations and other government “guidelines”

## Federal/State regulations / security requirements

- × FERPA (Family Educational Rights and Privacy Act)
- × CIPA (Children's Internet Protection Act)
- × PCI (Payment Card Industry)
- × Federal Circular A-123
- × FFIEC authentication in an electronic banking environment guidance
- × FISMA (Federal Information Security Management Act)
- × GLBA (Gramm-Leach Bliley Act)
- × HIPAA (Health Insurance Portability and Accountability Act)
- × Sarbanes-Oxley Act of 2002 (Public Company Accounting Reform and Investor Protection Act)
- × SB 1386 (California Information Practice Act)

## **FERPA (Family Educational Rights and Privacy Act)**

- The Family Educational Rights and Privacy Act of 1974 (FERPA or the Buckley Amendment) is a United States federal law codified at 20 U.S.C. § 1232g, with implementing regulations in title 34, part 99 of the Code of Federal Regulations. The regulations cover violations such as parent volunteers grading another child's work, school employees divulging information to someone other than the child's parents about a child's home-life, grades or behaviours, and school work posted on a bulletin board with a grade.
- This privacy policy also governs how state agencies transmit testing data to federal agencies. For example see Education Data Network.
- The act is also referred to as the Buckley Amendment, named for one of its proponents, Senator James Buckley of New York.

## **CIPA (Children's Internet Protection Act)**

- The Children's Internet Protection Act, also known as CIPA, is one of a number of bills that the United States Congress has proposed in an attempt to limit children's exposure to pornography and other controversial material on-line. Senator John McCain (R-AZ) introduced the bill that would become CIPA to the United States Senate in 1999. After various Representatives repeatedly introduced it to the United States House of Representatives, a final version cleared both houses and passed as part of an omnibus spending bill on December 15, 2000. President Bill Clinton signed it into law on December 21, 2000, and it was upheld by the Supreme Court of the United States on June 23, 2003 despite the American Library Association's attempt to have it declared unconstitutional.

[http://en.wikipedia.org/wiki/Children%27s\\_Internet\\_Protection\\_Act](http://en.wikipedia.org/wiki/Children%27s_Internet_Protection_Act)

## PCI Standard (Payment Card Industry)

- The Payment Card Industry (PCI) Data Security Standard was created by major credit card companies to safeguard customer information. Visa, MasterCard, American Express, and other credit card associations mandate that merchants and service providers meet certain minimum standards of security when they store, process and transmit cardholder data.

## Federal Circular A-123

- 1. Purpose and Authority. As Federal employees develop and implement strategies for reengineering agency programs and operations, they should design management structures that help ensure accountability for results, and include appropriate, cost-effective controls. This Circular provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls.
- The Circular is issued under the authority of the Federal Managers' Financial Integrity Act of 1982 as codified in 31 U.S.C. 3512.
- The Circular replaces Circular No. A-123, "Internal Control Systems," revised, dated August 4, 1986, and OMB's 1982 "Internal Controls Guidelines" and associated "Questions and Answers" document, which are hereby rescinded.

*<http://www.whitehouse.gov/omb/circulars/a123/a123.html>*

## FFIEC authentication in an electronic banking environment guidance

- On August 8, 2011, the FFIEC agencies issued guidance entitled Authentication in an Electronic Banking Environment (2011 Guidance). The 2011 Guidance focused on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services. Since 2001, there have been significant legal and technological changes with respect to the protection of customer information; 2 increasing incidents of fraud, including identity theft; and the introduction of improved authentication technologies. This updated guidance replaces the 2001 Guidance and specifically addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services.
- This guidance applies to both retail and commercial customers and does not endorse any particular technology. Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities.

[http://www.google.com/url?sa=t&ct=res&cd=1&url=http%3A%2F%2Fwww.ffiec.gov%2Fpdf%2Fauthentication\\_guidance.pdf&ei=ApvHRdy1Epm4iwHbm5CcDg&usg=\\_\\_EpTk9LMB9pJm8IZVbepTJTH7wQ0=&sig2=aa8www2f8hpoHgjXc3hHyQ](http://www.google.com/url?sa=t&ct=res&cd=1&url=http%3A%2F%2Fwww.ffiec.gov%2Fpdf%2Fauthentication_guidance.pdf&ei=ApvHRdy1Epm4iwHbm5CcDg&usg=__EpTk9LMB9pJm8IZVbepTJTH7wQ0=&sig2=aa8www2f8hpoHgjXc3hHyQ)

# FISMA (Federal Information Security Management Act)

- The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). The Act was meant to bolster computer and network security within the Federal Government and affiliated parties (such as government contractors) by mandating yearly audits.
- FISMA has brought attention within the Federal Government to cybersecurity, which had previously been much neglected. As of February 2005, many government agencies received extremely poor marks on the official report card, with an average of 67.3% for 2004, an improvement of only 2.3 percentage points over 2003.[1] This shows a marginal increase in how federal agencies prioritize cybersecurity, but experts warn that this average must increase for the Government to truly protect itself.

<http://en.wikipedia.org/wiki/FISMA>

## GLBA (Gramm-Leach Bliley Act)

- The Gramm-Leach-Bliley Act, also known as the Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (November 12, 1999), is an Act of the United States Congress which repealed the Glass-Steagall Act, opening up competition among banks, securities companies and insurance companies. The Glass-Steagall Act prohibited a bank from offering investment, commercial banking, and insurance services. The Gramm-Leach-Bliley Act (GLBA) allowed commercial and investment banks to consolidate. For example, Citibank merged with Travelers Group, an insurance company, and in 1997 formed the conglomerate Citigroup, a corporation combining banking and insurance underwriting services. Other major mergers in the financial sector had already taken place such as the Smith-Barney, Shearson, Pramerica and Travelers Insurance Corporation combination in the mid-1990's. This combination announced in 1993 and finalized in 1994 already violated the Glass-Steagall Act by combining insurance and securities companies. The law was passed to legalize these mergers. Historically, the combined industry has been known as the financial services industry

*<http://en.wikipedia.org/wiki/GLBA>*

# HIPAA (Health Insurance Portability and Accountability Act)

- The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996.
- According to the Centers for Medicare and Medicaid Services' (CMS) website, Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.
- Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.
- The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system.

<http://en.wikipedia.org/wiki/HIPAA>

## **Sarbanes-Oxley Act of 2002 (Public Company Accounting Reform and Investor Protection Act)**

- The Sarbanes-Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called SOX or Sarbox; July 30, 2002) is a United States federal law passed in response to a number of major corporate and accounting scandals including those affecting Enron, Tyco International, Peregrine Systems and WorldCom (recently MCI and currently now part of Verizon Businesses). These scandals resulted in a decline of public trust in accounting and reporting practices. Named after sponsors Senator Paul Sarbanes (D-Md.) and Representative Michael G. Oxley (R-Oh.), the Act was approved by the House by a vote of 423-3 and by the Senate 99-0.
- Jokingly referred to as the Auditors Continued Employment Act of '02

*[http://en.wikipedia.org/wiki/Sarbanes\\_Oxley](http://en.wikipedia.org/wiki/Sarbanes_Oxley)*

## **SB 1386 (California Information Practice Act)**

- California SB 1386 became effective in on 1st July 2003, amending civil codes 1798.29, 1798.82 and 1798.84.
- It requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed).
- The bill mandates various mechanisms and procedures with respect to many aspects of this scenario, subject also to other defined provisions.
- There are no exceptions to SB 1386 for companies whose home offices reside in other states or countries. Doing business with California residents is sufficient to make a company responsible to the law.

<http://www.sb-1386.com/>

# Risk Management

## The Classical Approach

*simply secure*

## Step One

### Current Year Assessment

- \* Explain need to management for a review of information security. Beg and plead for the financial support to perform said review.
- \* Issue an RFP (Request for Proposal) to a fixed number of vendors and Audit Firms.
- \* Review proposals and select the best candidates for performing the review.
- \* Receive word from managing body to select lowest bidder, which may or may not have been the best candidate from those petitioned for proposal.
- \* Contact lowest bidder and be informed there is a 6-8 month waiting period before the work can begin.
- \* Undergo the review
- \* Receive the report from the outside vendor or audit firm who performed the review.

## Step Two

### Current Year Remediation Effort

- × Two - Six months after assessment receive assessment report.
- × Review relevant findings and propose a remediation plan based on remediation steps offered by outside consulting firm.
  - × Those remediation steps which do not fit corporate culture or feasibility requirements can be either A) Ignored or B) crammed down corporate throat.
- × Beg for financial support to perform the remediation plan from upper management.
- × If needed bring in outside consulting firm for remediation effort.
  - × This will require an RFP, proposals and more begging for money.
- × Implement remediation plan and hope to keep it on schedule and on budget.
  - × If budget is exceeded remediation effort can be ended at any time, unless outside vendor has iron clad contract for remediation at which point the budget will escalate.

## Step Three

### Next Year

- × Repeat steps One and Two with increased budget.

### According to Insidesarbanesoxley.com:

- × In 2005 the estimated cost of compliance with Sarbane-Oxely alone was over \$ 5.8 billion with the same companies spending over 6 billion in 2006.
- × After 2005 36% of companies planned to increase spending, 52% planned to maintain spending levels and 12% hoped to decrease SOX spending.
- × Comprehensive numbers for 2006 have not been reported at this time.

*<http://www.insidesarbanesoxley.com/>*

# Failings of the Classical Approach

## Budgetary Constraints

- Increasing expenditures with little or no return of investment on an annual basis
- Small to mid-sized business can not keep up with the current compliance model as we know it without undergoing cuts.
- Financial constraints do not allow for mass expenditure on all relevant hardware devices necessary. If multiple devices are required for compliance it is possible the replacement cycle for new devices will expire prior to the complete purchase and implementation of all new hardware.
- Remediation efforts by outside consultants can exceed thousands of hours at high hourly rates. (Manager ABR is close to \$180/hr)

*[http://cpamanagement.blogspot.com/2006\\_08\\_01\\_archive.html](http://cpamanagement.blogspot.com/2006_08_01_archive.html)*

## Technology Constraints

- Hardware purchases may take time to implement if custom orders are needed or large mainframes are required.
- Some core operating software may not be compliant with regulations, requiring vendor updates or new software implementation
- Custom (home brewed) applications require significant time to rewrite or make compliant with regulations. Especially if change control processes are in place.
- It takes time to build expertise on new technologies and hiring experts is not always an option.

## Other Factors for Failure

- Lack of understanding by corporate board or employees regarding needed controls.
  - Often times mitigating controls or remediation steps are not properly explained by consultants
  - Often consultants do not properly explain the rationale for implementing controls.
- Cultural changes happen slowly over a long period of time, sometimes controls can try to change a corporate culture too fast and are rejected because of it.
- Lack of commitment by employees or the corporate board to make the change.
  - Most often this is caused by a misunderstanding of why changes need to be made or why certain regulations need to be adhered to.

## Evidencing the classic approach's failure

- In a study dated July of 2006 performed by GAO (12)
  - While the number of public companies announcing financial restatements from 2002 through September 2005 rose from 3.7 percent to 6.8 percent, restatement announcements identified grew about 67 percent over this period.
- In a recent report from the AICPA the following was observed (13)
  - The results suggested that well over half of the errors that resulted in restatements were caused by ordinary books and records deficiencies or by simple misapplications of the accounting standards. Approximately one-third of the errors related to situations in which there were one or more contributing factors from outside the company.
- InfoWorld Article from 1/17/2007 (14)
  - The TJX Companies, a large retailer that operates over 2,000 retail stores under brands such as Bob's Stores, HomeGoods, Marshalls, T.J. Maxx and A.J. Wright said on Wednesday that it suffered a massive computer breach on a portion of its network that handles credit card, debit card, check, and merchandise transactions in the U.S. and abroad.

- ITC Institute article (15)
  - Once More unto the Data Breach: Cold, Hard Costs of Data Exposure
    - What's untold is how much the episode is costing Company X, over and above the humiliation outlay. "Our estimate is that the cost ranges from \$25 to \$150 per impacted record," said Jon Oltsik, analyst at the Enterprise Strategy Group.
- Feb. 15, 2005 Choice Point (16)
  - Bogus accounts established by ID thieves. The initial number of affected records was estimated at 145,000 but was later revised to 163,000.
    - Update (1/26/06): ChoicePoint settled with the Federal Trade Commission for \$10 million in civil penalties and \$5 million for consumer redress.
    - Update (12/06/06): The FTC announced that victims of identity theft as a result of the data breach who had out-of-pocket expenses can now be reimbursed. The claims deadline is Feb. 4, 2007.
- Feb. 3, 2007 CTS Tax Service (16)
  - The computer and hard drive of a tax preparation company were stolen. Data included names, bank account numbers, routing numbers, birth dates, SSNs, and addresses.
    - This event is the 476<sup>th</sup> reported data breach since the Choice Point event
    - An estimated 101,070,850 individuals have had their information breached in the United States of America. Approximately one out of every three people.

# Take Ten Minutes

*simply secure*

# Welcome Back

*simply secure*

# Changing how we look at Compliance

## “Compliant” does not mean secure

- There is a misconception that if an organization is compliant with regulations they are secure.
  - A disturbing number of public entities make restatements because of internal process errors indicating a lack of adherence to procedures and security.
  - Public disclosures on information data breaches are on the rise, even at organizations compliant with regulations such as PCI, GLBA and HIPAA.
- Being compliant with regulations does not take into account best Risk Management strategies
  - The idea behind risk management is not to be compliant with regulations, but rather to manage an organizations risks. There is little to no benefit saying that an organization complied with the regulations if they have to alert the public to a data breach the day after their most recent audit is published.

## Why does this happen

- Regulations are written by lawmakers (or at least their staff)
  - Lawmakers are not the most technically savvy individuals on the face of the planet, they may have misconstrued ideas of data security which are not applicable to the real world.
  - The regulations tend to be vague enough to cause debate as to their interpretation.
  - There may be holes within the regulations which allow for an insecure setting to be compliant with the statute.
- PCI is the only exception to this formula, it was written by credit card company executives and consultants.
  - This standard appears to be the most effective in securing an environment as it includes firm standards and information security program.
  - The problem with PCI is the dictated report format is not usable by most information security shops.

## The cost of interpretation

- Sarbanes-Oxley compliance efforts 10-12 billion in 2005 and 2006
  - This amount is only anticipated to continue to rise as more companies struggle with compliance with SOX.
- An estimated 101,070,850 consumer's accounts breached
  - At \$25-\$150 per account that equals between \$2,526,771,250 and \$15,160,627,500 spent on Data Breaches in 2005 and 2006.
  - Those numbers do not take into account the reputation losses to the 476 organizations who have gone public with data breaches or the expenditures of being compliant with relevant regulations.
- PCI compliance costs have not been calculated but most organizations do little to nothing with the average 13,000 page compliance report as the information provided by scanning organizations is not easily utilized.
  - We can interpret this to mean that this is money down the drain in regards to securing information and managing risk for affected organizations.

## Closing the door on interpretation

- If we can change the course of risk management from interpretation of regulations to complying with hard standards we can better ensure the security of our client's information.
  - As the regulations often do not provide strict standards with little to no room for interpretation we need to look for security standards that do.
  - Adopting firm standards will save money in the long run as security standards are not open to interpretation and have a proven record of decreasing financial expenditures once implemented
  - If firm security standards are met a company will be 90% compliant with the relevant regulations automatically.

# Security Standards

a “New” way to approach Compliance

## Security Standards

- Information Security Standards have been around for a very long time.
  - Since accounting departments first adopted mainframes External Auditors have been setting the standards for security over them.
  - “Best Practices” have been around since the late eighties governing passwords and security settings as they evolved into the complex computing environment we now operate in.
- Dominant Security Standards in the Marketplace today
  - ISO 27001
  - COBIT
  - COSO

## ISO 27001

- ISO/IEC 27001 is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization and the International Electrotechnical Commission. Its full name is ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements but it is commonly known as "ISO 27001".
- ISO 27001 is a certification standard specifying requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS. The requirements are defined in a structured, formal format suitable for compliance certification.
- It is intended to be used in conjunction with ISO 17799, the Code of Practice for Information Security Management, which lists security control objectives and recommends a range of specific security controls. Organizations that implement an ISMS in accordance with the best practice advice in ISO 17799 are likely simultaneously to meet the requirements of ISO 27001, but certification is entirely optional.

[http://en.wikipedia.org/wiki/ISO\\_27001](http://en.wikipedia.org/wiki/ISO_27001) (17)

## Strengths of the ISO 27001 Standard

- Highly detailed technical requirements
- Internationally accepted
- Overall comprehensive standard over policies and procedures
- Little room for interpretation
- Provides excellent assurances over information security.
- Is a “standalone” standard for data security and integrity.

## Weaknesses of the ISO 27001 standard

- Not widely utilized or understood by public accounting firms or auditors in the United States.
- Not written in a format easily understood by audit and risk management departments.
- Corporate awareness of the standard is limited due to structure of the standard.
- Can require a major change in corporate culture.
- Can be regarded as expensive to implement.

## COBIT

- The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992.
- COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.
- The first edition was published in 1996; the second edition in 1998; the third edition in 2000 (the on-line edition became available in 2003); and the fourth edition in December 2005. It has more recently found favor due to external developments, especially after the Enron scandal with the subsequent passage of the Sarbanes-Oxley Act.
- In its 4th edition, COBIT has 34 high level objectives that cover 215 control objectives categorized in four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

<http://en.wikipedia.org/wiki/Cobit> (18)

## Strengths of the COBIT standard

- Widely utilized by public accounting firms and auditors in the United States.
- Corporate awareness is high regarding COBIT.
- The standard allows for some customization across diverse industries.
- Can be integrated into different corporate cultures more easily.
- Provides comprehensive guidelines for policies and procedures
- Compliments control structure of COSO

## Weaknesses of the COBIT standard

- Does not go into great detail regarding the technical configuration of technology.
- Interpretation of the standard can vary between audit and public accounting firms.
- Often misrepresented to executives
- Because of its close ties to SOX audits it is often perceived as costly to implement and maintain.
- Is not seen as a “standalone” standard for data security and integrity because of its affiliation with COSO in the public accounting firms.

## COSO

- Committee of Sponsoring Organizations of the Treadway Commission (COSO), is a U.S. private-sector initiative, formed in 1985. Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence. COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.
- COSO is sponsored and funded by 5 main professional accounting associations and institutes; American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives Institute (FEI), The Institute of Internal Auditors (IIA) and The Institute of Management Accountants (IMA).

<http://en.wikipedia.org/wiki/COSO> (19)

## Strengths of the COSO standard

- Time tested and widely set as the standard for financial reporting controls in the United States and abroad.
- COSO is already widely adhered to within the corporate environment.
- Complimented by the control structure of COBIT

## Weaknesses of the COSO standard

- Does not provide details on technical implementation of information technology.
- Relies heavily on manual controls over data flow and transaction reporting.
- Deals only with data processing of financial statements.
- Is not a “standalone” standard for data security and Integrity as it does not take IT controls into account outside of the financial records.

# Risk Management

moving forward

*simply secure*

## Realign our Focus & Message

- Instead of being concerned if our clients are “compliant” we need to focus on if they are secure.
- By explaining the risk associated with a vulnerability there is a better chance remediation steps will be understood and taken.
- By basing our approach on securing their environment versus complying with a regulation we can help our clients save money.
- Risk is derived from real world events and is best explained in those terms. If we can not explain a problem realistically it won't be taken seriously.

- There is no silver bullet to security, but “we” can improve the security of client networks through hard and fast standards.
- Adoption of Security Standards shows a dedication to Risk Management.
- Security Standards are written expressly to ensure compliance with regulations while best securing an environment, we do not need to reinvent the wheel.
- There is a Security Standard for every one- they just need to find the right one.

# a few take aways

## Ten things “We” need to remember

1. We should not take pleasure in discovering control gaps
2. We are there to help improve our client's data security and control environment.
3. Our clients can always choose another firm next year so respect them.
4. Implementing a security standard at an client will improve our reputation and make future sales easier.
5. Just because a client is “compliant” it does not mean that “our” firms opinion will not be questioned if there is a data breach.

6. Our reputations depend on our clients ability to implement our recommendations.
7. Fear, uncertainty, and doubt (FUD) is not an appropriate way to make recommendations or finding fault in a control structure.
8. If a client is resistant to our recommendations it is up to them to accept that risk if they wish.
9. We need to represent our recommendations better because they are often misunderstood.
- 10. Security leads to compliance, not the other way around.**

## Ten things clients need to remember

1. Risk Management is not about being compliant it is about Managing Risk
2. Just because a company complies with a regulation it does not mean that company is securing its data.
3. Risk Management need not be an expensive endeavour.
4. Cultural changes to bring security to the fore front of each employee's day have to occur.
5. The days of burying security breaches is long over.

6. Audits are a friendly events.
7. Consultants and Auditors are not there to cost them their job or make them look stupid.
8. Although we act like we know everything we don't, but we do know someone who does.
9. “We” are trying to help them!
10. There really are bad people out there trying to get their proprietary information, “we” are not just being paranoid.

## Shavlik's 10 most encountered Security Problems

1. Lack of an Intrusion Prevention System (IPS)
2. Lack of configuration standards for desktops and workstations.
3. Lack of up to date Antivirus software
4. Lack of protection against spyware / malware
5. Allowing end users to run as local administrator, which invites them to make security decisions for the entire company.

6. Failure to require users to utilize strong passwords with uppercase, lowercase, numeric and symbolic characters .
7. The infamous quote “There is no patch for human stupidity” applies to everyone, i.e. lack of training for all levels of management and employees.
8. Failure to take an inventory of all Information Technology Assets and keep it up to date
9. Failure to utilize total disk encryption on all laptops, PDAs and Smart Phones to better protect the organization’s information.
10. Failure to follow proper patching procedures “Patch, Patch, Patch a little more and then when you think you are completely patched -- patch again.”

# Q & A

*simply secure*

## Sources

- 1) <http://en.wikipedia.org/wiki/FERPA>
- 2) [http://en.wikipedia.org/wiki/Children%27s\\_Internet\\_Protection\\_Act](http://en.wikipedia.org/wiki/Children%27s_Internet_Protection_Act)
- 3) <http://www.whitehouse.gov/omb/circulars/a123/a123.html>
- 4) <http://www.google.com/url?sa=t&ct=res&cd=1&url=http%3A%2F%2Fwww.ffiec.gov%2F>
- 5) <http://en.wikipedia.org/wiki/FISMA>
- 6) <http://en.wikipedia.org/wiki/GLBA>
- 7) <http://en.wikipedia.org/wiki/HIPAA>
- 8) [http://en.wikipedia.org/wiki/Sarbanes\\_Oxley](http://en.wikipedia.org/wiki/Sarbanes_Oxley)
- 9) <http://www.sb-1386.com/>
- 10) <http://www.insidesarbanesoxley.com>
- 11) [http://cpamanagement.blogspot.com/2006\\_08\\_01\\_archive.html](http://cpamanagement.blogspot.com/2006_08_01_archive.html)
- 12) <http://www.gao.gov/cgi-bin/getrpt?GAO-06-678>
- 13) CPCAF Alert #155 – December 29, 2006
- 14) [http://www.infoworld.com/article/07/01/17/HNtjxbreach\\_1.html](http://www.infoworld.com/article/07/01/17/HNtjxbreach_1.html)
- 15) <http://www.itcinstitute.com/display.aspx?id=2328>
- 16) <http://www.privacyrights.org/ar/ChronDataBreaches.htm>
- 17) [http://en.wikipedia.org/wiki/ISO\\_27001](http://en.wikipedia.org/wiki/ISO_27001)
- 18) <http://en.wikipedia.org/wiki/CobIT>
- 19) <http://en.wikipedia.org/wiki/COSO>