
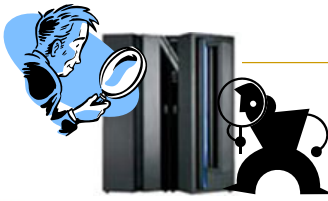



1st European IBM / GSE Conference 2007
for z/VSE, z/VM and Linux on System z

Auditing and Compliance in a z/VSE-z/VM Shop



Copyright © 2007 illustro Systems International, LLC



Agenda

- Regulations, Regulations
 - PCI-DSS
 - Basel2
 - MiFID
 - ISO/IEC 27799
 - "SOX"
 - HIPAA, GLBA, etc. etc.
- What motivated the regulations?
- Solutions and Best Practice – a primer



This is no way meant to be an exhaustive list of a way of ensuring you are compliant with any regulations.
It's not even an exhaustive list of all the regulations, let alone how to be compliant.
This is intended to be a primer on the concept of regulations, and we cannot even guarantee
that it is an exhaustive primer.
If any of these were true, we'd all be exhausted.
Certified under Regulation 2.678-IBM 2007



Copyright © 2007 illustro Systems International, LLC

IBMGSE2007-2

Copy of Presentation

→illustro.com/conferences



Copyright © 2007 illustro Systems International, LLC

IBMGSE2007-3

PCI - DSS



- **Payment Card Industry – Data Security Standards**
 - Developed by major credit card companies
 - Guideline to help companies prevent fraud, hacking and other issues
 - Any company which processes, stores or transmits credit card numbers must be PCI-DSS compliant



Copyright © 2007 illustro Systems International, LLC

PCI – DSS...

- Originally began as 5 different programs
 - VISA Information Security Program
 - MasterCard Site Data Protection
 - American Express Data Security Operating Policy
 - Discover Information and Compliance
 - JCB Data Security Program
- 15 December 2004 common causes aligned their policies and published PCI-DSS
- September 2006 standard was updated to 1.1



Copyright © 2007 illustro Systems International, LLC

PCI – DSS...

The control objectives and their requirements are:

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



Copyright © 2007 illustro Systems International, LLC

Basel II

- Second accord of the Basel Committee on Banking Supervision- members of G10
- Purpose is to create an international standard that banking regulators can use when creating regulations about risks bank face
- Aimed at the banking industry
 - Architected under a "3 Pillar Concept"
 - (1) minimum capital requirements (addressing risk),
 - (2) **supervisory review – guard against internal and external fraud**
 - (3) market discipline – to promote greater stability in the financial system.

See The Light.

Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-7

MiFID

- **Markets in Financial Instruments Directive**
 - Introduces a single regulatory regime for investment services across the European Economic Area (27 member states + Iceland, Norway and Lichtenstein)
 - Cornerstone of European Commission's Financial Services Action Plan
 - 3 Objectives
 - To complete the process of creating a single EU market for investment services
 - To respond to changes and innovations which have occurred in securities markets
 - **To protect investors by making markets deeper, more competitive and more robust against fraud and abuse**

See The Light.

Copyright © 2007 illustro Systems International, LLC



ISO/IEC 27799

- Information Security Standard from International Organization for Standardization (*Organisation internationale de normalisation*)
- Provides guidance to health organizations and other holders of personal health information on how to protect such information
- 12 point standard
 - Health information systems should provide audit trails that:
 - Allow the identification of all system users who have accessed or modified a given patient's record(s) over a given period of time
 - Allow the identification of all patients whose records have been accessed or modified by a given system user over a given period of time.
 - Read access should be included in the audit trail

See The Light.

Copyright © 2007 illustro Systems International, LLC




**Illustro**
SYSTEMS INTERNATIONAL, LLC
See The Light.™

Copyright © 2007 illustro Systems International, LLC

Page 3

Sarbanes-Oxley: a/k/a "SOX"

- Signed into U.S. law on July 30th, 2002
- Named after U.S. Senator Paul Sarbanes D-MD, and U.S. Representative Michael Oxley R-OH
- Introduced significant changes in financial reporting and mandates for publishing information



illustro
See The Light.[™]

illustro Systems International, LLC

IBMGSE2007-10

SOX...

- Introduced following a number of high profile U.S. corporate failures



Adelphia **WORLD.COM**
ENRON


illustro
See The Light.[™]

Copyright © 2007 illustro Systems International, LLC

IBMGSE2007-11

SOX...

- "deter and punish corporate and accounting fraud and corruption, ensure justice for wrongdoers, and protect the interests of workers and shareholders"




illustro
See The Light.[™]



Copyright © 2007 illustro Systems International, LLC

IBMGSE2007-12

SOX...



- Organized into 11 "titles"
- Section 404 causes the most concern because of rules governing public disclosure
 - Makes managers responsible for maintaining an "adequate internal control structure and procedures for financial reporting";
 - Demands that companies' auditors "attest" to the management's assessment of these controls and disclose any "material weaknesses"
 - Strong new criminal penalties await transgressors.
- Remarkable because of notoriety and media attention

© 2007-13


Cost of SOX...



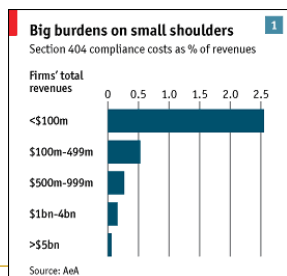
- Companies paid an average of \$2.4m more for their most recent audits than anticipated
- Deloitte says large firms spent nearly 70,000 man hours complying with the new laws
- Windfall for the accounting/audit industry
- Less visible costs, e.g. some companies are de-listing; foreign firms not listing on U.S. exchanges

Copyright © 2007 illustro Systems International, LLCIBM GSE 2007-14

Cost of SOX...



- Burden on smaller firms more dramatic



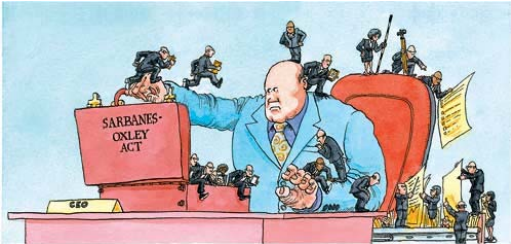
Big burdens on small shoulders
Section 404 compliance costs as % of revenues


Firms' total revenues	Compliance costs as % of revenues
<\$100m	~2.5%
\$100m-499m	~1.0%
\$500m-999m	~0.5%
\$1bn-4bn	~0.2%
>\$5bn	~0.1%

Source: AEA

Copyright © 2007 illustro Systems International, LLCIBM GSE 2007-15

Cost of SOX





See The Light.™

Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-16

SOX...

- High emphasis on financial reporting and corporate governance
- But implications for security, information protection and control management
- Security is a strong theme in SOX
- Most are modeling their responses on ISO17799
 - Very important standards related to information security



See The Light.™

Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-17

SOX...






See The Light.™

Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-18

HIPAA




- Not HIPPA (or Hippo!)
- **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct
- U.S. Department of HHS – enacted in 1996, initial deadline for providers – 2002
- Intended to improve Medicare process through standard transmission
 - This introduced privacy issues
- Who must comply (Covered Entities)?
 - Health Care Providers (who transmit electronic transactions covered by the HIPAA regulations)
 - Health Plans (self insured/insured, HMOs, health insurance companies, employer health plans, and similar arrangements)
 - Health Care Clearinghouses

illustro
See The Light.[™]

Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-19

HIPAA – What It Mandates




- **Privacy** - provides new rules in regard to how an individual's health information may be used and disclosed by covered entities.
- **Transaction and Code Sets** - requires the use of standard transaction formats and code sets when an individual's financial health information is transmitted electronically by a covered entity for purposes of payment, coverage determinations, eligibility determinations, and similar business matters.
- **Security** - requires covered entities to have specific security measures in place to protect an individual's health information that is sent or stored electronically.
- Also carries civil and criminal penalties for non-compliance

illustro
See The Light.[™]

Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-20

HIPAA - Costs




- Estimates vary “slightly”
 - Overall costs to comply with HIPAA
 - \$5.8 billion from the government agency in charge of the regulation
 - \$43 billion from the Blue Cross-Blue Shield Association.
- Some analysts say it will cost more than Y2K conversion work


illustro
See The Light.[™]

Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-21


HIPAA - Costs






2007-22

HIPAA Information Concerns



- Many software and hardware vendors promote the ability to achieve "HIPAA compliance"
 - Technology is only an enabler, cannot make compliant
- Requires:
 - Basic technology to adequately encrypt, authenticate or identify communication partners
 - Effective password-key management system when transmitting health-related information.
 - Reporting in the event of non-compliance
- Misconception that it bans some methods, e.g. PDAs and email



Copyright © 2007 illustro Systems International, LLC

IBMGSE2007-23

GLBA






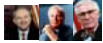
- The Gramm-Leach Bliley Act
- a/k/a The Financial Modernization Act of 1999
- Protect consumers personal financial information held by financial institutions



Copyright © 2007 illustro Systems International, LLC

IBMGSE2007-24

GLBA...





- GLBA gives authority to 8 federal agencies and the states to enforce:
 - Financial Privacy Rule: governs the collection and disclosure of customers' personal financial information by financial institutions
 - The Safeguards Rule: requires all financial institutions to design, implement and maintain safeguards to protect customer information.

illustro
See The Light.[™]

Copyright © 2007 illustro Systems International, LLC IBMGSE2007-25

Some Others...




- FERPA - Family Educational Rights and Privacy Act
 - Parent's rights over students data
 - Rights transfer when student is 18
 - Cannot give parent information without student consent
- COPPA - Children's Online Privacy Protection Act
 - Give parents control over what information is collected from their children online and how such information may be used.

illustro
See The Light.[™]

Copyright © 2007 illustro Systems International, LLC IBMGSE2007-26

California – Privacy Legislation



- Any company that sells a product or service to a California resident, even if the company is based outside the state, may be affected.
- Just having a website that a California resident visits—and one out of 10 Americans lives in California—can put you under the jurisdiction of these laws.


illustro
See The Light.[™]

Copyright © 2007 illustro Systems International, LLC IBMGSE2007-27

California – Privacy Legislation...

- Identity theft driving the paranoia
 - Estimated 10 million Americans experienced I/T last year
 - Aberdeen group estimated losses could reach \$2 trillion worldwide
- California passed SB 168
 - Prevented businesses from using SSN as identifiers
 - IBM last year required its more than 100 health insurance providers to stop printing Social Security numbers on medical ID cards, claims forms and other documents or risk losing their business
 - The change affected more than 540,000 IBM retirees, employees and their families in the United States

"But he that filches from me my good name/Robs me of that which not enriches him/And makes me poor indeed." - Shakespeare, Othello, act iii. Sc. 3.




illustro
See The Light.[™]

Copyright © 2007 illustro Systems International, LLC IBM GSE 2007-28

Information, Information

- All regs are motivated by the same phenomena
 - Internet suddenly (literally) connected millions of heretofore separate systems, and billions of people
 - Vast quantity of information suddenly available
 - Common access (Web) and other methods made it relatively easy to obtain




illustro
See The Light.[™]

Copyright © 2007 illustro Systems International, LLC

The Formerly Accepted was Suddenly Very, Very Bad

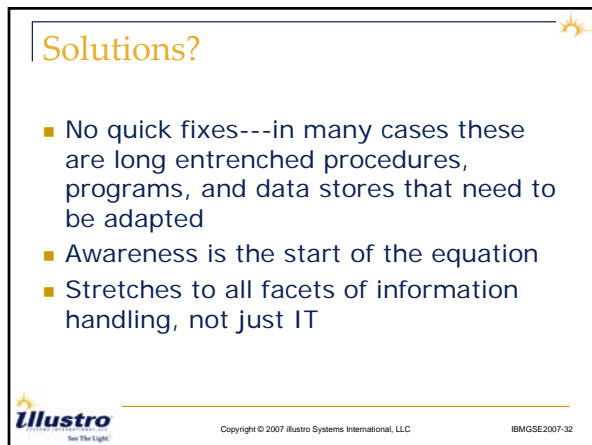
- Procedures that were de facto for decades became audit violations
 - Social Security Numbers as ID (military/schools/medical)
 - IT backup tapes sent off site
 - All "insiders" (employees, internal users) were doing what they were supposed to
 - Even affected non-IT procedures
 - No more telephone information
 - Fax authorization forms

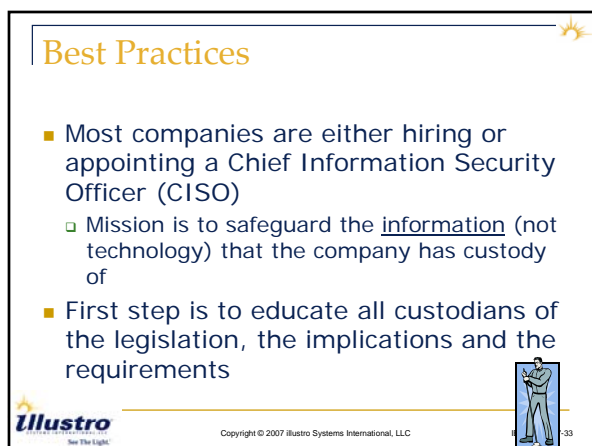


illustro
See The Light.[™]


Copyright © 2007 illustro Systems International, LLC IBM GSE 2007-30







Best Practices...



- Review and document information flow
 - Entry points and requirements, e.g.
 - Is critical information required for identification, e.g. SSN?
 - Is data sent over clear links on public networks?
 - Exit points and requirements, e.g.
 - Are required authorizations obtained before releasing information?
 - Are recipients authenticated adequately?
- Publish a Privacy Policy (Information handling)
- Monitor for breaches; if in doubt, NOTIFY

illustro
See The Light.[®]

Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-34

Best Practices...

- From an IT perspective, many areas:
 - Consider ways of centralizing your data---oh, wait, you're on a mainframe!!
 - Much easier to manage, audit, enact policies, control access
 - Others are seeing the "benefits" of centralized data and application control
 - www.citrix.com
 - Review backup policies, and actual results
 - Backups are NOT valid unless tested in restore

illustro
See The Light.[®]

Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-35

Best Practices...



"IT'S JUST UNTIL WE GET BACK UP ON THE INTERNET."

illustro
See The Light.[®]

IBM GSE 2007-36

Best Practices...

- Define and enforce access control policies through security software
 - Commercial security packages
 - Offer access, control and audit
 - For VSE – at least BSM and ACLR
- Explore technology to record session data
 - Can be used for triggers/alerts
 - Also for replay for audit, investigations, pattern detection
- Review encryption:
 - Needs
 - Wants
 - Budget




See The Light.™

Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-37

Best Practices...

- Encryption has many possible “touchpoints”
 - Encrypted data at rest
 - Encrypted data at the field level for sensitive data, e.g. SSN
 - Encrypted data over the wire (e.g. SSL)
- Any data that leaves the confines of the physical data center should be encrypted
 - Offsite backup tape data
 - FTP data being transmitted ANYWHERE on public network
 - Screen traffic (Web, Telnet etc.)
 - Email data (Outlook has free encryption capability)
 - Instant Messenger Data
 - Print data (consider online print access only)
 - Laptop data
 - USB drive data




See The Light.™


Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-38

A “Healthy Paranoia”



- Abundant activity has brought to light many weaknesses
- Rethink traditional processes
- Look for information “leakage”
- React when you find it, but be sure to notify all appropriate parties
- Assume abuse – internal and external
- Review, Respond and Repeat



See The Light.™

Copyright © 2007 illustro Systems International, LLC

IBM GSE 2007-39

