

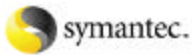


## Regulatory Compliance

*Impact on Information Security Programs*



Bruce W. Moulton  
VP – Information Security Business Strategy  
January 12, 2005



### Disclaimer ...

- ▶ I am a senior information security professional.
- ▶ I am not a lawyer
- ▶ Therefore, this is not legal or regulatory advice.

The information contained in this presentation is made available for informational purposes only and is not legal advice. The information is provided only as general information which may or may not reflect the most current legal developments. This information is not intended to constitute legal advice or to substitute for obtaining legal advice from an attorney licensed in your state.

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s. Copyright © 2003 Symantec Corporation. All rights reserved.





## Agenda

---

- 1 Specific Regulatory "Hot-Buttons"
- 2 General Regulatory Requirements/Impacts
- 3 The "Right" Thing To Do
- 4 Summary and Conclusions
- 5 Symantec Solutions
- 6 Discussion



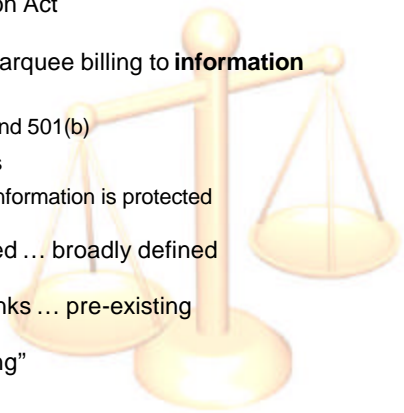
1

## Specific Regulatory "Hot Buttons"



## Quick Overview

**GLBA**

- ▶ Financial Services Modernization Act
  - ▶ Privacy sections give explicit marquee billing to **information security**
    - In the law ... sections 501(a) and 501(b)
    - In the guidelines and standards
    - Non-public personal financial information is protected
  - ▶ All financial institutions regulated ... broadly defined
  - ▶ Meaningful enforcement for banks ... pre-existing
  - ▶ Other enforcement still “maturing”
- 

## Specific Regulatory Requirements

**GLBA – Title V Section 501(a)**

*“It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ non-public personal information.”*

NOTE: “Financial Institution” is broadly defined

## Specific Regulatory Requirements

**GLBA – Title V Section 501(b)**

*“ ... each agency or authority ... shall establish appropriate standards for the financial institutions ... relating to administrative, technical and physical safeguards –*

1. *to ensure 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.”*

## Specific Regulatory Requirements

**GLBA ... Hot-Buttons from the Law**

## 501 (a):

- ▶ “Affirmative and Continuing” ... a process not an event
- ▶ “Security and Confidentiality” ... security explicitly highlighted
- ▶ “Non-public Personal Information” ... clear information scope
- ▶ “Financial Institution” very broadly defined ... broad, clear applicability

## 501(b):

- ▶ “Administrative, Technical and Physical” ... not just IT Security
- ▶ “Security and Confidentiality” ... security highlight reinforced
- ▶ “Anticipated Threats and Hazards” ... duty to be informed and respond
- ▶ “Unauthorized Access” ... time-honored foundation stone of security

Specific Regulatory Requirements

## GLBA .... Hot-Buttons From the Guidelines (ref OCC 12 CFR Part 30)

- ▶ Information Security Program ... written, approved, managed
- ▶ Board of Directors ... must be involved
- ▶ Risk Assessment ... foundation for choice of controls
- ▶ Manage and Control Risk ... based on risk assessment
  - 8 Recommended security measures
  - Training
  - Test controls
- ▶ Third-party Service Provider Arrangements
- ▶ Adjust the Program ... duty to learn, adapt and be dynamic
- ▶ Report to the Board ... close the loop

Specific Regulatory Requirements

## GLBA - The 8 Recommended Security Measures

1. **Access** controls on customer information **systems**
2. **Access** restrictions at **physical** locations with customer information
3. **Encryption** of electronic customer information
4. Procedures for customer information **system modifications**
5. Dual control procedures, **duty segregation**, background checks
6. **Monitoring** systems to detect actual/attempted attacks
7. **Response** Programs for suspected or detected attacks
8. Measures to protect against **environmental hazards**

## Quick Overview

**SOX**

- ▶ “To protect investors by improving the **accuracy and reliability** of corporate disclosures”
  - Periodic (e.g. quarterly) and annual reports
- ▶ **Accountability** by corporate officers, public auditors, attorneys
  - Accountability through **Personal Liability**
  - Personal **signatures** on management’s assertions
- ▶ **Public Auditors** will review management’s assertions
- ▶ **Internal Controls** are explicitly recognized as a **foundation** of information accuracy and reliability
  - **Information Security Controls** are not mentioned in the law

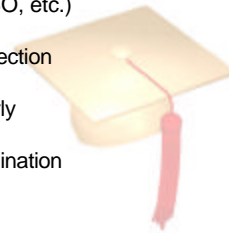
## Specific Regulatory Requirements

**SOX ... SEC Final Rules**

- ▶ Each company must **choose and declare an accepted framework** of internal control ...
  - COSO specifically cited by SEC as compliant
  - Committee of Sponsoring Organizations (Treadway Commission)
- ▶ **IT Controls** prominent in COSO but non-specific
- ▶ **COBIT®** ... Provides IT specifics (IT Governance Institute)
  - ISACA strongly suggests COBIT® for IT SOX compliance
- ▶ **Information Security Controls** prominent in COBIT®

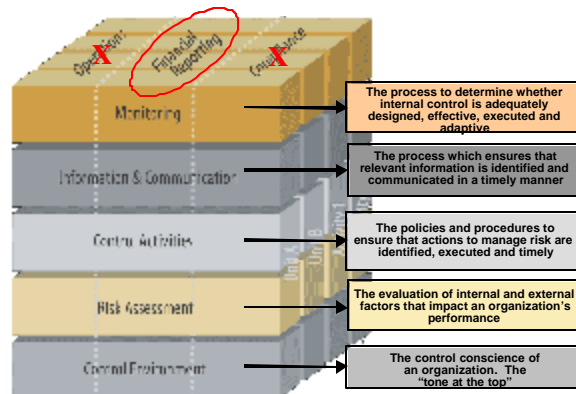
Specific Regulatory Requirements  
**SOX ... Hot-Buttons**

- ▶ Personal Accountability ... and criminal penalties
- ▶ Scope Definition ...
  - We know it is all about publicly reported financial information.
  - What is financially relevant information? Relevant processes?
  - What is meant by "internal controls"?
- ▶ Control Framework? COSO ... CobiT ... Other (ITIL, ISO, etc.)
- ▶ Role of IT and Information Security ... making the connection
- ▶ Informing Sr. Management re state-of-control ... regularly
- ▶ Informing Auditors re state-of-control ... at time of examination



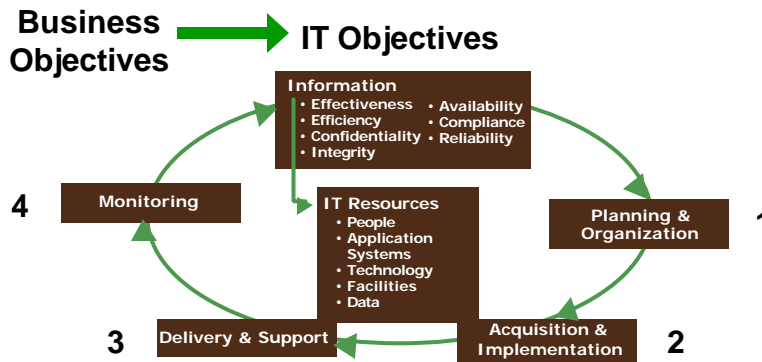
SOX - Frameworks of Control

**COSO** (www.coso.org)



**COSO Internal Controls – Integrated Framework**

(Source: COSO and Deloitte & Touche)



Domains further decomposed into **34 Key Control Processes**

Source: ITGI, ISACA & META Group

**MONITORING**

- M1 Monitor the processes
- M2 Assess internal control adequacy
- M3 Obtain independent assurance
- M4 Provide for independent audit

**DELIVERY & SUPPORT**

- DS1 Define service levels
- DS2 Manage third-party services
- DS3 Manage performance and capacity
- DS4 Ensure continuous service
- DS5 Ensure systems **security**
- DS6 Identify and attribute costs
- DS7 Educate and train users
- DS8 Assist and advise IT customers
- DS9 Manage the configuration
- DS10 Manage problems and incidents
- DS11 Manage data
- DS12 Manage facilities
- DS13 Manage operations

**PLANNING & ORGANIZATION**

- PO1 Define a strategic IT plan
- PO2 Define the information architecture
- PO3 Determine the technological direction
- PO4 Define the IT organization and relationships
- PO5 Manage the IT investment
- PO6 Communicate management aims and direction
- PO7 Manage human resources
- PO8 Ensure compliance with external requirements
- PO9 Assess risks
- PO10 Manage projects
- PO11 Manage quality

**ACQUISITION & IMPLEMENTATION**

- AI1 Identify solutions
- AI2 Acquire and maintain application software
- AI3 Acquire and maintain technology architecture
- AI4 Develop and maintain IT procedures
- AI5 Install and accredit systems
- AI6 Manage changes

Source: ITGI, ISACA & META Group

SOX - Frameworks of Control

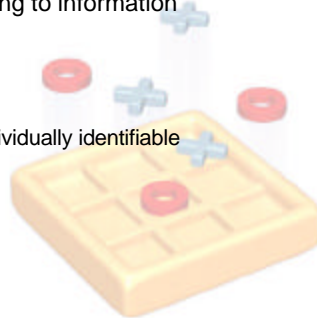
## COBIT® ... DS5 – Ensure System Security (21 Secondary Processes)

- |      |   |      |   |
|------|---|------|---|
| 5.1  | Manage Security Measures                            | 5.12 | Re-accreditation  |
| 5.2  | Identification, Authentication, and Access          | 5.13 | Counterparty Trust  |
| 5.3  | Security of Online Access to Data                   | 5.14 | Transaction Authorization                                   |
| 5.4  | User Account Management                             | 5.15 | Non-Repudiation   |
| 5.5  | Management Review of User Accounts                  | 5.16 | Trusted Path  |
| 5.6  | User Control of User Accounts                       | 5.17 | Protection of Security Functions                            |
| 5.7  | Security Surveillance                               | 5.18 | Cryptographic Key Management                                |
| 5.8  | Data Classification                                 | 5.19 | Malicious Software Prevention, Detection, and Correction    |
| 5.9  | Central Identification and Access Rights Management | 5.20 | Firewall Architectures and Connections with Public Networks |
| 5.10 | Violation and Security Activity Reports             | 5.21 | Protection of Electronic Values                             |
| 5.11 | Incident Handling                                   |      |   |

Quick Overview

## HIPAA

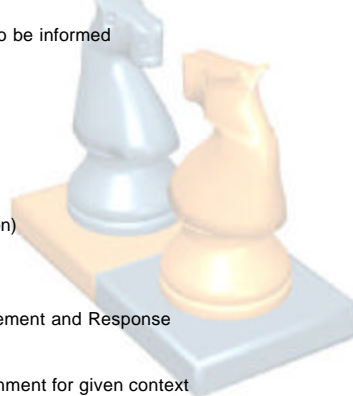
- ▶ Law seeks to encourage efficiency of health information processing ... e.g. insurance claims
- ▶ Privacy focus gives explicit marquee billing to information security (similar to GLBA)
  - In the law
  - In the guidelines and standards
  - Protected health information (PHI) ... individually identifiable
- ▶ All who handle PHI are regulated
- ▶ So far, enforcement is complaint-driven



Specific Regulatory Requirements

**HIPAA ... Hot-Buttons from the Standards (selected)**

- ▶ “Administrative, Technical and Physical” ... not just IT Security
- ▶ “Anticipated Threats and Hazards” ... duty to be informed
- ▶ C, I and A
- ▶ Risk Assessment
- ▶ Access Management
- ▶ Network Security (transmission ... encryption)
- ▶ Intrusion Detection (both network and host)
- ▶ Malicious code detection -- Incident Management and Response
- ▶ In other words ... a complete control environment for given context

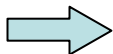


Specific Regulatory Requirements

**Security and Privacy Compliance (HIPAA)**

**Examples of covered entities that must implement these standards**

- Health Plans
- Health Care Providers
- Health Care Clearing Houses
- Health Care Product Manufacturers (in some cases)
- Public Health Authorities
- Life Insurer
- Employer
- Schools and Universities



**“Create or receive past, present or future Protected Health Information”**

## Quick Overview

**California Breach 1386**

- ▶ Driven by increasing identity theft rate
- ▶ Creates obligation to **notify** information subject/owner if certain data is accessed by unauthorized parties in unencrypted form (“safe harbor” for encryption)
- ▶ California enforcement is currently complaint-driven
- ▶ Same concept in discussion at Federal level
  - Diane Feinstein ... Senate 1350
  - Extensions to GLBA guidelines and standards (FFIEC)

## Specific Regulatory Requirements

**CA 1386 ... Hot-Buttons**

- ▶ **Notification ...**
  - You can only notify if you know a breach has happened!
  - AND private notification is vastly preferred ... must know who!
- ▶ **Encryption ...**
  - In storage AND in transit
  - Crypto strength not specified
  - Crypto is necessary but not sufficient



## Quick Overview

**VISA and MasterCard**

- ▶ Driven by VISA/MC goals to be seen as secure AND by how they see their regulatory duties as financial institutions.
- ▶ Criteria established for merchants and participating banks
  - VISA Cardholder Information Security Program (CISP)
  - MasterCard Site Data Protection Program (SDP)
- ▶ First enforcement appears to be with large “retail” merchants (hotels, national chain stores, oils, etc.)

## Specific Regulatory Requirements

**VISA CISP ... Hot-Buttons**

1. Install and maintain a working **firewall** to protect data
2. Keep security **patches** up-to-date
3. Protect stored data
4. **Encrypt** data sent across public networks
5. Use and regularly update **anti-virus** software
6. Restrict **access** by “need to know”
7. Assign unique ID to each person with computer access
8. Don't use vendor-supplied defaults for passwords and security parameters
9. Track all access to data by unique ID
10. Regularly **test** security systems and processes
11. Implement and maintain an information security **policy**
12. Restrict **physical access** to data



Specific Regulatory Requirements  
**MasterCard SDP ... Hot-Buttons**

1. Security Management
2. Access Control
3. Operational Security
4. Application and System Development
5. Network Security
6. Physical Security



2

General Regulatory  
Requirements/Impacts



## General Regulatory Requirements

**Measurement and Monitoring**

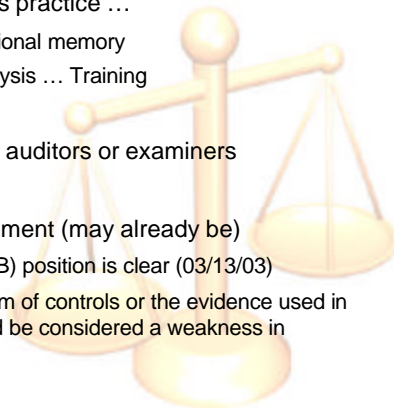
- ▶ “What gets measured gets done ... “
- ▶ “What gets measured is compliant ...”
- ▶ If you are not measuring it, it is probably not compliant ...
  - and you certainly don’t know its status ...
  - as you are required to do!
- ▶ If you must comply ... (with policy or law or standard)  
Then, you must measure!



## General Regulatory Requirements

**Documentation and Reporting**

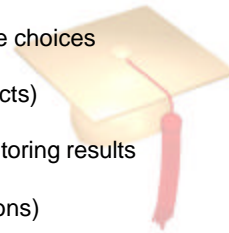
- ▶ Besides being a sound business practice ...
  - Inform management ... Institutional memory
  - Business and/or technical analysis ... Training
- ▶ Arguably the best way to inform auditors or examiners
- ▶ Likely to be a regulatory requirement (may already be)
  - Auditing Standards Board (ASB) position is clear (03/13/03)
  - “Failure to document the system of controls or the evidence used in making the assessment should be considered a weakness in internal control”



General Regulatory Requirements

**Things To Document**

- ▶ Security architecture ... related to broader IT architecture
- ▶ Information risk assessment
- ▶ IT resources that require security controls
- ▶ The intended security control environment
- ▶ The chosen controls ... And the logic behind those choices
- ▶ Security processes and procedures (people aspects)
- ▶ The security monitoring processes --Security monitoring results
- ▶ Control status and incidents/events (with resolutions)



General Regulatory Impacts

**Cost of Compliance**

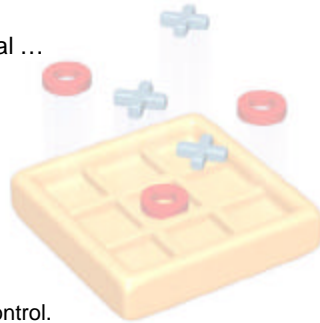
- ▶ It Depends ...
  - On where you start; and
  - On where you "set the bar"
- ▶ Minimal to Monumental Impact Range
- ▶ Budget Accordingly



## General Regulatory Impacts

**Compliance With What ?**

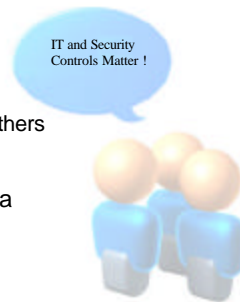
- ▶ “We got what we asked for ...”
  - “appropriate to size and scope...” (GLBA)
  - Required vs addressable ... (HIPAA)
- ▶ Laws and standards are relatively general ...
  - The laws give general guidance; but
  - Control choices are very specific
  - Self-Definition Is Required.
- ▶ Simple process, but hard work
  - Say what you intend to do, and
  - Do what you said you would do, and
  - Show that you really know the state-of-control.



## General Regulatory Impacts

**Who Is Judging Your Compliance?**

- ▶ Who Is Your Auditor ?
  - IT control weaknesses may or may not generate a qualified opinion
  - Some believe IT controls are key; but
  - Others accept mitigating controls.
- ▶ Who Is Your Regulatory Examiner ?
  - Some are more technically experienced than others
- ▶ Understand Your Auditor's/Examiner's Criteria



## The “Right” Thing To Do



The “Right” Thing To Do

### The Regulatory & Standards “Climate”

- Gramm-Leach-Bliley Act (**GLBA**)
- Sarbanes-Oxley Act (**SOX**)
- Health Insurance Portability & Accountability Act (**HIPAA**)
- California Breach Notification Act (**SB 1386**) ... + Federal Level
- Basel Capital Accord II (**Basel II**)
- NERC Urgent Action Standard 1200 (**NERC 1200**)
- Homeland Security Act (**HSA**)
- USA Patriot Act (**USA-PA**)
- Corporate Information Security Accountability Act of 2003 (**Putnam**)
- Visa and MasterCard Security Programs (**VISA CISP, MC SDP**)
- **ISO 17799 and BS 7799**
- And Others ... (EU DPD, PEPIDA, pending Spy Act, etc.)

Each with clear or potential information security impact ...

The "Right" Thing To Do

## The Good News

- ▶ Security (by-and-large) is Security ...
- ▶ GOOD ... Solving one regulatory compliance security challenge should position you to solve others much more easily.
- ▶ BETTER ... If you gather ALL your regulatory security challenges together, **you can solve them with one comprehensive security program!**
- ▶ BEST ... You already have a good security program and are already compliant !

Finally ... Some Good News!



The "Right" Thing To Do

## Complete Program "Required" ...

- ▶ A Sound, Balanced Program Is Required !
  - No single silver bullet ... Need a full clip
  - C – I – A
  - People ... Process ... Technology
  - Physical and Logical
  - End-to-end control
  - Risk-based control choices
- ▶ AT LEAST Covering Regulated Information Domains



The "Right" Thing To Do

## Elements of a Complete Program

1. Reflect organizational security objectives in policy and standards
2. Assign roles/responsibilities and organize resources
3. Know what information you have and who it belongs to
4. Know what information is sensitive and why (C, I, A)
5. Know what threatens the information you hold
6. Know where the information is/goes (flows) and what form it is in
7. Define the degree of protection required and/ or justified
8. Evaluate/ design, procure/ develop, implement, operate, and maintain controls that satisfy the above requirements AND monitor the control environment AND report status to management
9. Detect attacks, respond to those that succeed and recover operations
10. Learn, adjust, adapt ... train and communicate



4

## Summary and Conclusions



## Summary and Conclusions

**The Key Points**

- ▶ You can not achieve privacy without security
- ▶ You can not achieve integrity/accuracy without security
- ▶ You can not be in control without good security
- ▶ A complete, balanced, risk-based, **standards-based** information security program that embraces all the protected information classes is your best compliance strategy
- ▶ A “culture of compliance” should also be “persuasive”



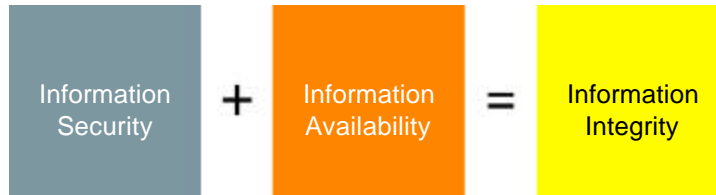
5

Symantec Solutions



Symantec Solutions

## The Symantec “Information Integrity” Message



Information that is secure, but not available to your people is worthless.

Information your people can get to, but that is insecure, is suspect. And so is everything they do with it.

Information that has integrity — security plus availability — is more trustworthy. And trustworthy information is worth more.

Symantec Solutions

## Symantec Solutions for Increased Compliance (Examples)

- ▶ **Duty to Be Informed** ... DeepSight + MSS for early warning
- ▶ **Risk Assessment** ... Consulting, ESM
- ▶ **Measure, Monitor and Document** ... ESM to measure platform compliance, SSMS+SESA
- ▶ **Respond** ... Symantec LiveState, SSMS incident management
- ▶ **Encrypt** ... Symantec VPN capabilities
- ▶ **A Complete Program** ... Everything Symantec sells can help! Early warning, firewalls, VPN, anti-virus, intrusion detection, vulnerability assessment, content filtering, anti-spam, discovery-provisioning-backup-recovery, consulting services, managed services, platform compliance monitoring, patch management, honey pots (and more...)
  - As point solutions or as appliances



6

Discussion



Thank You



Bruce W. Moulton  
bruce\_moulton@symantec.com