The Information Security Standards Marketplace

Richard Baskerville
Visiting Professor
Bocconi University

Rather than just a technical decision subject to regulatory requirements, IT security standards adoption is a decision taken in a complex marketplace of competing standards, competing service providers, competing security design methods, and competing national and international legislative requirements, all under the oversight of closely watched audit firms and government regulators. The audit dependence on standards in this market inverts the economic decisions for internal controls in information systems. Without regulatory standards, risk economics are necessary to justify acquisition and implementation of controls. With regulatory standards, risk economics are necessary to justify exceptions to the acquisition and implementation of controls. The impact of this economic shift may drive down organizational competitiveness or increase misleading compliance behaviour among IT professionals.

Outline

1. The Information Security Standards Marketplace
2. Competing National And International Legislative Requirements
3. Competing Standards And Competing Service Providers
4. Audit Firms And Government Regulators
5. Reoriented Security Design Methods

The Information Security Standards Marketplace

Public Company Audit Reforms

Restore Investor Confidence in Capital Markets
- Significant changes to securities laws or practices
- The wake of corporate financial scandals
  - Enron
  - Arthur Andersen
  - WorldCom
- European Union Council 8th Directive (Expansion)
- Sarbanes-Oxley Act of 2002 (US)
- Corporate Law Economic Reform Program (CLERP 9) (Australia)
### EU 8th Directive

- Establishes a new audit regulatory committee composed of member states and chaired by a representative of the European Commission (EC). The committee will assist the EC in establishing the implementation measures of the directive.
- Auditors or audit firms must:
  - Be approved and registered in any member state.
  - Meet continuous education requirements.
  - Subject to robust professional ethics.
  - Be independent from the audited company.
  - Adhere to the International Standards on Auditing.
  - Meet quality assurance standards.
  - Be governed by the member state system of investigation and sanctions.
  - Be subject to public oversight.
  - Follow relationship procedures with an audited entity.
  - Disclose an internal governance statement.
  - Cooperate with the mandated audit committee in financial reporting.

### US: Sarbanes-Oxley Act of 2002 (107 H.R. 3763)

**Enhanced Financial Disclosures**
- Title IV (Sections 401-409)
- Deals with company responsibilities for periodic financial reports, assessment of internal controls, code of ethics, and other aspects of disclosures.
- Section 404: Management Assessment Of Internal Controls.
  - Requires an “internal control report”
    - Establish and maintain adequate internal control structure and procedures
    - Assess their effectiveness

### Public Company Accounting Oversight Board

**Title I (Sections 101 - 109)**

Deals with the establishment of PCAOB that registers and reviews Public Accounting Firms under the oversight of SEC, with responsibility for investigations and disciplinary actions for breeches of accounting standards.

### Auditor Independence

**Title II (Sections 201-209)**

- Deals with conflicts of interest in business relationships of audit firms and steps to unveil such conflicts, like rotating firms and audit partners, reporting to audit committee, etc.
- Section 201: Services Outside The Scope Of Practice Of Auditors; Prohibited Activities.
  - This section outlaws an audit firm that provides “non-audit service” to companies during audits, e.g.,
    - Bookkeeping
    - Financial information systems design and implementation
    - Management functions or human resources

### Corporate Responsibility

**Title III (Sections 301-308)**

Deals with company audit committees, and conduct all of officers and directors.

### Enhanced Financial Disclosures

**Title IV (Sections 401-409)**

- Deals with company responsibilities for periodic financial reports, assessment of internal controls, code of ethics, and other aspects of disclosures.
- Section 404: Management Assessment Of Internal Controls.
  - Requires an “internal control report”
    - establish and maintain adequate internal control structure and procedures
    - assess their effectiveness
Analyst Conflicts of Interest
Title V (Section 501)
Deals with conflict of interest rules for exchanges and associations.

Commission Resources and Authority
Title VI (Sections 601-604)
Deals with budget and authority.

Studies and Reports
Title VII (Sections 701-705)
Deals with government reports.

Corporate and Criminal Fraud Accountability
Title VIII (Sections 801-807)
Deals with faked or destroyed documents, retention of records, and criminal penalties.

White Collar Crime Penalty Enhancements
Title IX (Sections 901-906)
Increases some criminal penalties, criminalizes record tampering and fraudulent financial statements, etc.

Corporate Tax Returns
Title X (Section 1001)
CEO must sign tax returns
Deals with record tampering, impeding officials, and SEC authority to freeze payments and exclude securities fraudsters as company officers.

Corporate Fraud and Accountability

Title XI (Sections 1101-1107)

Business processes are now dependent on IT

The IT function is crucial

Compliance means
- Internal control must map to IT systems
- IT systems risks must be reported
- IT controls must be tested

Impact on IT

What has this got to do with information systems?

IT “Sabotage”

Bad IT will screw this thing up

Lack of domain knowledge, insular IT culture, and lack of internal control knowledge combine to create significant weaknesses in controls and systems developed by IT. (Cannon & Growe, Journal of Corp. Accounting & Finance, 2004)

CIO Involvement

(PWC Guidance)

Avoiding IT Problems

Better utilize internal audit
Adopt comprehensive control framework
Raise risk awareness of IT workers
Train IT on internal control
Include IT on SOX planning committees
Loan IT workers to functional departments

Avoiding IT Problems

Outsource IT
- Weak company staff
- Multiple IT platforms
- Management dissatisfaction with internal IT
- Internal politics interferes
- Train CPAs to advise clients on outsourcing of IT
- When to outsource
- Where to outsource

Avoiding IT Problems

Or .... Avoiding IT Problems


Or .... Avoiding IT Problems

Austalian CLERP 9
- Ethical purpose similar to Sarbox & EU 8, but softer
- Based on disclosure rather than criminalization
- Regulates auditor independence, periodic reporting, and corporate disclosure and certification of financial reports
- Two systems are similar enough to permit parallel compliance
  - SarbOx compliance increases overhead
  - Some issues in attorney-client confidentiality
- Executives are not required to certify the maintenance of internal controls to the public
  - Required to certify to the directors of the company that the financial statements comply with accounting standards and represent the true and fair view of the current financial position of the company

Extra-Territorial Law
- The more restrictive legislative framework effectively override national regulatory authorities in other countries
- SarbOx taking precedence over CLERP 9 in parallel compliance situations for companies subject to US SEC regulations.
- Can extend to outsourcing vendors where controls subject to SarbOx compliance reporting

Impact: Emerging IT Risk Management Practices
Developed in an industry study
- Define an overall organizational risk management strategy
- Adhere to one of the prevalent IT security standards
- Develop and deploy safeguards and controls that provide the optimal combination of risk treatments
- Provide system risk review mechanisms
- Test all risk treatments

Adhere to One of the Prevalent IT Security Standards
- Encodes an overall IT security architecture
- Critically consider controls and safeguards inventory
- E.g., risk analysis to eliminate unnecessary safeguards
- Standard -- risk analysis dialectic

Competing Standards And Competing Service Providers

Guidance and Standards: Examples
Provide assurance and evidence that proper and responsible measures are present in the organization's systems.
- Technical Standards
  - ISO/IEC 17799,
- Professional Standards
  - COBIT (Control Objectives for IT), a generally applicable and accepted standard for good information technology security and control practices in organizations.
- Qualification Criteria
  - ITSEC, TCSEC, Common Criteria
- Industry Practices and Standards
  - NIST 800-12 Computer Security Handbook
  - Payment Card Industry (PCI) Standard
  - ITIL (IT Infrastructure Library)
Technical Standards

Example: ISO/IEC 17799

Risk Assessment & Treatment

ISO 17799

- The objectives of this section are:
  - To establish a process for identifying major security threats and vulnerabilities and determine the potential impact within the context of an organization’s business objectives and strategies.

Plan Do Act Check

ISO 17799

Security Policy

ISO 17799

- The objectives of this section are:
  - To provide management direction and support for information security.
The objectives of this section are:
- To manage information security within the Company.
- To maintain the security of organizational information processing facilities and information assets accessed by third parties.
- To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

The objectives of this section are:
- To reduce risks of human error, theft, fraud or misuse of facilities;
- To ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work;
- To minimise the damage from security incidents and malfunctions and learn from such incidents.

The objectives of this section are:
- To ensure the correct and secure operation of information processing facilities;
- To minimise the risk of systems failures;
- To protect the integrity of software and information;
- To maintain the integrity and availability of information processing and communication;
- To ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
- To prevent damage to assets and interruptions to business activities;
- To prevent loss, modification or misuse of information exchanged between organizations.

The objectives of this section are:
- To control access to information;
- To prevent unauthorised access to information systems;
- To ensure the protection of networked services;
- To prevent unauthorized computer access;
- To detect unauthorised activities;
- To ensure information security when using mobile computing and tele-networking facilities.

The objectives of this section are:
- To ensure security is built into operational systems;
- To prevent loss, modification or misuse of user data in application systems;
- To protect the confidentiality, authenticity and integrity of information;
- To ensure IT projects and support activities are conducted in a secure manner;
- To maintain the security of application system software and data.

The objectives of this section are:
- Establish security incident reporting processes that ensure prompt reporting;
- Ensure that incidents lead to corrective actions;
- Establish security event escalation processes;
- Establish contractor and third party reporting processes.
The objectives of this section are:
- To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

The objectives of this section are:
- To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
- To ensure compliance of systems with organizational security policies and standards
- To maximize the effectiveness of and to minimize interference to/from the system audit process.

The objectives of this section are:
- To prevent unauthorised access, damage and interference to business premises and information;
- To prevent loss, damage or compromise of assets and interruption to business activities;
- To prevent compromise or theft of information and information processing facilities.

The objectives of this section are:
- To maintain appropriate protection of corporate assets
- To ensure that information assets receive an appropriate level of protection.

This standard has evolved toward the development of management systems for information security and provides a stronger basis for third party audit and certification. It offers a managerially-oriented complement to the technologically-oriented ISO 17799.
Industry Practices & Standards

Examples:
- NIST 800-12
- PCI
- ITIL

NIST Computer Security Division

http://csrc.nist.gov/publications/nistpubs/
- SP 800-12 An Introduction to Computer Security: The NIST Handbook, October 1995
- SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
- SP 800-33 Underlying Technical Models for Information Technology Security, December 2001
- SP 800-34 Contingency Planning Guide for Information Technology Systems, June 2002
- SP 800-65 Integrating Security into the Capital Planning and Investment Control Process, January 2005

NIST SP 800-14 Reference Model

OECD's Guidelines for the Security of Information Systems
- Accountability - The responsibilities and accountability of owners, providers and users of information systems and other parties...should be explicit.
- Awareness - Owners, providers, users and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures...for the security of information systems.
- Ethics - The Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interest of others are respected.
- Multidisciplinary - Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints.
- Proportionality - Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm...
- Integration - Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security.
- Timeliness - Public and private parties, at both national and international levels, should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.
- Reassessment - The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.
- Democracy - The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.
Payment Card Industry Data Security Standard

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

ITIL

IT Infrastructure Library

- Best practices and guidelines for managing information technology services
- Integrated, process-based approach
- Originated as a 1980's UK government drive
- Focus on quality, efficient, cost-effective delivery of IT services

Major ITIL Volumes

- Software asset management
- Service support
- Service delivery
- Planning to implement service management
- ICT infrastructure management
- Application management
- Security management
- The business perspective

ITIL Structure

<table>
<thead>
<tr>
<th>Process Areas</th>
<th>Strategic Level</th>
<th>Tactical Level</th>
<th>Operational Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Release management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service-level management</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ITIL Security

- Security Management Products
  - Policies
  - Processes
  - Procedures
  - Work instructions

Audit Firms And Government Regulators
Audit Firms And Government Regulators

- SarbOx-driven audit firms reviewing assessment processes for internal controls
  - Was ISO/IEC 17799 or CobiT the better choice?
  - Firms cannot consult, only review
- PCAOB an indirect factor: ensuring that organizational decisions about standards adoption are made independently from an external auditor.

Security Design Context of Risk Analysis

So many safeguards . . .
We can't afford to include all of them . . .
But which?

Generic Security Design Model

Second Generation Methods

1. Identify and evaluate system assets
2. Identify and evaluate threats
3. Identify possible controls
4. Risk analysis
5. Prioritize controls for implementation
6. Implement and maintain controls

Security Design Model Example: Octave

Octave
Carnegie Mellon Software Engineering Institute

- Operationally Critical Threat, Asset, and Vulnerability Evaluation
- Considers both organizational and technological issues
- Focused on organizational strategy and practice
- Driven by operational risks and security practices
Octave Process

(From Christopher Allies, Audrey Donalde, James Stevens, Carol Woody, Introduction to the OCTAVE® Approach, August 2003, Software Engineering Institute, http://www.cert.org/octave/pubs.html)

Octave Method

- Phase 1: Build Asset-Based Threat Profiles
  - Process 1: Identify Senior Management Knowledge
  - Process 2: Identify Operational Area Knowledge
  - Process 3: Identify Staff Knowledge
  - Process 4: Create Threat Profiles
- Phase 2: Identify Infrastructure Vulnerabilities
  - Process 5: Identify Key Components
  - Process 6: Evaluate Selected Components
- Phase 3: Develop Security Strategy and Plans
  - Process 7: Conduct Risk Analysis
  - Process 8: Develop Protection Strategy

Risk Analysis and Standards: Opposing Approaches

- Risk analysis
  - Default decision: adopt no safeguards
  - Risk analysis economically justifies adoption of safeguard
- Standards
  - Default decision: adopt all safeguards
  - Justify in audit decisions not-to-adopt safeguard

The Information Security Standards Marketplace

The Information Security Standards Marketplace

Richard Baskerville
Visiting Professor
Bocconi University

Conclusion

Rather than just a technical decision subject to regulatory requirements, IT security standards adoption is a decision taken in a complex marketplace of competing standards, competing service providers, competing security design methods, and competing national and international legislative requirements, all under the oversight of closely watched audit firms and government regulators. The audit dependence on standards in this market inverts the economic decisions for internal controls in information systems. Without regulatory standards, risk economics are necessary to justify acquisition and implementation of controls. With regulatory standards, risk economics are necessary to justify exceptions to the acquisition and implementation of controls. The impact of this economic shift may drive down organizational competitiveness or increase misleading compliance behaviour among IT professionals.