Ethical Guidelines for Information Use

Dr. Dang Tran Khanh

Dept. of CSE/HCMUT

khanh@cse.hcmut.edu.vn

Outline

- Introduction
- Control of information: PAPA
- Security and controls
- IT Governance and Security
- SOX 2002
- Summary

Introduction: Core learning objectives

- List and define PAPA and why it is important
- Identify the issues related to the ethical governance of information systems
- Understand security issues of organizations and how organizations are bolstering security
- Describe how security can be best enacted
- Define the Sarbanes-Oxley Act and the COBIT framework

Theory	Definition	Metrics
Stockholder	Maximize stockholder wealth, in legal and non-fraudulent manners.	Will this action maximize stockholder value? Can goals be accomplished without compromising company standards and without breaking laws?
Stakeholder	Maximize benefits to all stakeholders while weighing costs to competing interests.	Does the proposed action maximize collective benefits to the company? Does this action treat one of the corporate stakeholders unfairly?
Social contract	Create value for society in a manner that is just and nondiscriminatory.	Does this action create a "net" benefit for society? Does the proposed action discriminate against any group in particular, and is its implementation socially just?

Figure 9.1 Three normative theories of business ethics.

Outline

- Introduction
- Control of information: PAPA
- Security and controls
- IT Governance and Security
- SOX 2002
- Summary

Privacy

- Possessing the “best” information and knowing how to use it will be the winner
- However, keeping this information safe and secure is a high priority (see Figure 9.2)
- Privacy – “the right to be left alone”
- Managers must be aware of regulations that are in place regarding the authorized collection, disclosure and use of personal information

Area	Critical Questions
Privacy	What information must a person reveal about one's self to others? What information should others be able to access about you – with or without your permission? What safeguards exist for your protection?
Accuracy	Who is responsible for the reliability and accuracy of information? Who will be accountable for errors?
Property	Who owns information? Who owns the channels of distribution, and how should they be regulated?
Accessibility	What information does a person or an organization have a right to obtain, under what conditions, and with what safeguards?

Figure 9.2 Mason's areas of managerial concern.

Accuracy

- Managers must establish controls to insure that information is accurate
- Data entry errors must be controlled and managed carefully (e.g., wrong bill payment information)
- Data must also be kept up to date
- Keeping data as long as it is necessary or legally mandated is a challenge

Property

- Mass quantities of data are now stored on clients
- Who owns this data and has rights to it are questions that a manager must answer
- Managers must understand the legal rights and duties accorded to proper ownership

Accessibility

- Access to information systems and the data that they hold is paramount
- Users must be able to access this data from any location (if it can be properly secured and does not violate any laws or regulations)
- Major issue facing managers is how to create and maintain access to information for society at large
  - This access needs to be controlled to those who have a right to see and use it (identity theft)
  - Also, adequate security measures must be in place on their partners end

PAPA and Managers

- Managers must work hard to implement controls over information highlighted by PAPA
- Limit access to data – avoid identify theft, and respect customer's privacy
- FTC (the US Federal Trade Commission) requires more disclosure of how companies use customer data
  - Gramm-Leach-Bliley Act (1999)
- Information privacy guidelines must come from above: CEO, CFO, etc.

Outline

- Introduction
- Control of information: PAPA
- Security and controls
- IT Governance and Security
- SOX 2002
- Summary

Security and Controls

- PAPA principles work hand-in-hand with security and controls
- Executives reported that hardware/software failures, and major viruses, had resulted in unexpected or unscheduled outages of their critical business systems (Ernst & Young)
- Technologies have been devised to manage the security and control problems (see Figure 9.3), e.g.: RFID (Radio Frequency Identification) is being used to control access and manage assets
- Employees require proper training and education

IT Governance and Security

- Figure 9.4 shows an appropriate governance pattern for each decision
  1. Information Security Strategy
  2. Information Security Policies
  3. Information Security Infrastructure
  4. Information Security Education/Training/Awareness
  5. Information Security Investments
- The archetypes clearly define the responsibilities of the major players in the company

Information Security Decision	Recommended Archetype	Rationale
Information Security Strategy	Business monarchy	Business leaders have the knowledge of the company's strategies, upon which security strategy should be based. No detailed technical knowledge is required
Information Security Policies	IT duopoly	Technical and security implications of behaviors and processes need to be analyzed and tradeoffs between security and productivity need to be made. Need to know the particularities of company's IT infrastructure.
Information Security Infrastructure	IT monarchy	In depth technical knowledge and expertise is needed.
Information Security Education/Training/ Awareness	IT duopoly	Business buy-in and understanding are needed; Technical expertise and knowledge of critical security issues is needed in building programs.
Information Security Investments	IT duopoly	Requires financial (quantitative) and qualitative evaluation of business impacts of security investments. Business case has to be presented for rivaling projects.

Figure 9.4 – Matching information security decisions and archetypes

Outline

- Introduction
- Control of information: PAPA
- Security and controls
- IT Governance and Security
- SOX 2002
- Summary

Sarbanes-Oxley Act of 2002

- The Sarbanes-Oxley (SoX) Act of 2002 was enacted to increase regulatory visibility and accountability of public companies and their financial health
  - All companies subject to the SEC are subject to the requirements of the act
  - CEO's and CFO's must personally certify and be accountable for their firm's financial records and accounting
  - Firms must provide real-time disclosures of any events that may affect a firm's stock price or financial performance
  - IT departments realized that they played a major role in ensuring the accuracy of financial data (Sec 404)

IT Control and Sarbanes-Oxley

- In 2004 and 2005 IT departments began to identify controls, determined design effectiveness, and validated operation of controls through testing
- Five IT control weaknesses were uncovered by auditors:
  1. Failure to segregate duties within applications, and failure to set up new accounts and terminate old ones in a timely manner
  2. Lack of proper oversight for making application changes, including appointing a person to make a change and another to perform quality assurance on it
  3. Inadequate review of audit logs to not only ensure that systems were running smoothly but that there also was an audit log of the audit log
  4. Failure to identify abnormal transactions in a timely manner
  5. Lack of understanding of key system configurations

Frameworks for Implementing SoX

- **COSO -** Committee of Sponsoring Organzations of the Treadway Commission
  - Created three control objectives for management and auditors that focused on dealing with risks to internal control
    - **Operations** – to help the company maintain and improve its operating effectiveness and protect the assets of shareholders
    - **Compliance** – to assure that the company is in compliance with relevant laws and regulations.
    - **Financial reporting** – to assure that the company's financial statements are produced in accordance with Generally Accepted Accounting Principles (GAAP).
  - Five essential control components were created to make sure a company is meeting its objectives

Frameworks

- COBIT (Control Objectives for Information and Related Technology)
  - IT governance framework that is consistent with COSO controls
  - Issued in 1996 by Information Systems Audit & Control Association (ISACA)
  - Figure 9.5 lists the components of COBIT and examples of each component

Component	Description	Example
Domain	One of four major areas of risk (Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate); Each domain consists of multiple processes	Delivery and Support
Control Objective	Focuses on control of a process associated with risk; There are 34 processes	DS (Delivery and Support) 11 - Manage Data: ensures delivery of complete, accurate and valid data to the business
Key Goal Indicator	Specific measures of the extent to which the goals of the system in regard to a control objective have been met	“A measured reduction in the data prepartion process and tasks”
Key Performance Indicator	Actual, highly-specific measures of the for measuring accomplishment of a goal	“Percent of data input errors” (Note: the percentage should decrease over specified periods of time)
Critical Success Factor	Describes the steps that a company must take to accomplish a Control Objective. There are 318 Critical Success Factors.	“Data entry requirements are clearly stated, enforced and supported by automated techniques at all level, including database and file interfaces”
Maturity Model	A uniquely-defined six-point ranking of a company’s readiness for each control objective made in comparison with other companies in the industry	“Data is not recognized as a corporate resource and asset. There is no assigned data ownership or individual accountability for data integrity and reliability. Data quality and security is poor or non-existent”

Figure 9.5 – Components of COBIT and their examples

IT and the Implementation of Sarbanes Oxley Act Compliance

- Section 404 of SoX deals with management's assessment of internal controls making implementation considerable
- CIO works with auditors, CFO, and CEO
  - CIO must tread carefully
  - Braganza and Franken provide six tactics for working effectively in these relationships (Fig 9.6)
  - The extent to which a CIO could employ these various tactics depends upon the power that he or she holds relating to the SoX implementation

Tactic	Definition	Examples of Activities
Knowledge Building	Establishing a knowledge base to implement SoX	Acquiring technical knowledge about SoX and 404
Knowledge Deployment	Disseminating knowledge about SoX and developing an understanding of this knowledge among management and other organizational members	Moving IT-staff with knowledge of 404 to parts of the organization that are less knowledgeable Creating a central repository of 404 knowledge Absorbing 404 requriements from external bodies Conducting training programs to spread an understanding of SoX
Innovation Directive	Organizing for implementing SoX and announcing the approach	Issuing instructions that encourage the adoption of 404 compliance practices Publishing progress reports of each subsidiary's progress toward 404 implementation Putting drivers for 404 implementation in place Directing 404 implementation from top down and/or bottom up
Mobilization	Persuading decentralized players and subsidiaries to participate in SoX implementation	Creating a positive impression of SoX (and 404) implementation Conducting promotional and awareness campaigns
Standardization	Negoitating agreements between organizational members to facilitate the SoX implementation	Using mandatory controls, often embedded within the technology, to which users must comply Indicating formal levels of compliance or variance from prescribed controls Establishing standards of control throughout the organization Creating an over-arching corporate compliance architecture
Subsidy	Funding implements' costs during the SoX implementation and users' costs during its deployment and use	Centralizing template development Developing web-based resources Investing in developing the skills of IT staff to implementing 404 Funding short-term skill gaps Investing in tracking implementation Managing funds during implementation to achieve specific IT-related 404 goals.

Figre 9.6 CIO Tactics for implementing SoX compliance

Other Control Frameworks

- ISO
  - ISO (International Organization for Standardization) is the world's **largest developer** and publisher of **International Standards**
- Information Technology Infrastructure Library (ITIL)
  - Set of concepts and techniques for managing IT
  - Offers 8 sets of management procedures

Summary

- Introduction
- Control of information: PAPA
- Security and controls
- IT Governance and Security
- SOX 2002
  - Frameworks for implementation section 404
- Summary
- Next lecture:
  - Chapter 10 (short introduction)