# Chapter 8
# Governance of the Information Systems Organization

*Jason C. H. Chen, Ph.D.*
*Professor of MIS*
*School of Business Administration*
*Gonzaga University*
*Spokane, WA 99258*
*chen@jepson.gonzaga.edu*

---

## Today's Business Environment

- We are all familiar with the rapid pace of change we are seeing now in large part due to the emergence of the e-business economy and Internet time. Business life cycles are getting shorter and shorter and we are all struggling to adapt our organizations and business process to cope with that change.

---

## Three Necessary Perspectives

- **Business Environment** **External**
- **Enterprises Environment** **Internal**
- **IT Environment** **Internal & Technology**

**Business Success**

TM -3

---

## Information, Organization, and Control

- "The important point is that technology neither encourages nor discourages centralized or decentralized structures and controls, but …

  offers new possibilities."

N

---

## Information System Strategy Triangle

### Strategy Triangle

**Business (Firm) Strategy**

**Where** is the business going and why?

*Direction for business*
*Supports business*

*IT impact and potential*

**Organizational Strategy**  ←  Needs and priorities  →  **IS/IT Strategy**

*Infrastructure and services*

**What** is required?

**How** it can be delivered?
1. Architecture/Infrastructure,
2. MIS Organization (sourcing and IT governance)
3. Funding
4. Project Management

---

## Learning Objectives

- Understand *how* governance structures define the *way* decisions are made in an organization.
- Describe the three models of governance based on *organization structure* (centralized, decentralized, and federal), *decision rights*, and *control* (e.g., COSO, COBIT, ITIL).
- Discuss examples and strategies for implementation.

## Real World Example

- In April 2011, Sony was hit by one of the biggest **data breaches** in history when PlayStation was hacked.
- Compromised the personal information of potentially 100 million users.
- Sony took the on-line platform offline for weeks.
- To woo back its customers, it offered a "welcome back package."
  - Free games, movies, and $1 million *identity theft insurance policy* per customer.
- Estimated cost of the breach was 104 million British pounds—not counting reputational damage.
- A U.S. Congressional Committee, the U.K. Minister of Culture, and the city of Taipei were among those demanding more information about the breach.

## Real World Example (Cont.)

- In September 2011, Sony posted its new **security policy and standards** on its website.
- Appointed a former official at the U.S. Department of Homeland Security as its first Chief Information Security Officer.
  - Responsible for assuring the security of Sony's information assets and services.
  - Oversees corporate information security, privacy, and Internet safety.
  - Coordinates closely with key headquarters groups on security issues.
- A **governance** structure helps Sony's security professionals, IS organization, and business units work toward achieving corporate goals, which now include *information security*.

## IT Governance

- **Governance** in the context of business enterprises is all about making decisions that *define expectations*, *grant authority,* or *ensure performance*.
  - Aligning behavior with business goals through empowerment and monitoring.
- **Empowerment** comes from granting the right to make decisions.
- Monitoring comes from evaluating performance.
- IT governance focuses on how *decision rights* can be distributed differently to facilitate centralized, decentralized, or hybrid modes of decision making.
- The *organizational structure* plays a major role.

## Centralized vs. Decentralized Organizational Structures

- **Centralized**: reduces duplication since resources under one control and, often, in one location.
- **Decentralized**: creates flexibility because resources not in the same location or control
- *"Federalism"* combines centralization with decentralization (Figure 8.1 shows the continuum of where these structures fall.)
- Companies with higher levels of governance *maturity* have a need for control that is made possible in the **centralized** structure.
- For example:
  - Bethlehem Steel allows major business units (plants) to *decentralize* and operate independently
  - Levi-Strauss *centralized* to minimize the duplication of resources and save on costs.

## Figure 8.1  Organizational continuum

Decentralization   **Federalism**   Centralization

## Organizational Structural Approaches

- Figure 8.2 shows advantages and disadvantages of each organizational approach.
- Most companies want to achieve the advantages derived from both organizational paradigms.
- **Federalism** is a structuring approach that distributes power, hardware, software, data, and personnel between a central IS group and IS in business units.
- A **hybrid** approach enables organizations to benefit from both structural approaches.
- Figure 8.3 shows how these approaches interrelate.

## Figure 8.2 Advantages and disadvantages of organizational approaches.

| Approach | Advantages | Disadvantages | Companies Adopting |
|---|---|---|---|
| Centralized | • Global standards and common data<br>• "One voice" when negotiating supplier contracts<br>• Greater leverage in deploying strategic IT initiatives<br>• Economies of scale and a shared cost structure<br>• Access to large capacity<br>• Better recruitment and training of IT professionals<br>• Better control of security and databases<br>• Consistent with centralized enterprise structure | • Technology may not meet local needs<br>• Slow support for strategic initiatives<br>• Schism between business and IT organization<br>• Us versus them mentality when technology problems occur<br>• Lack of business unit control over overhead costs | Zara<br>UPS[3] |
| Decentralized | • Technology customized to local business needs<br>• Closer partnership between IT and business units<br>• Greater flexibility<br>• Reduced telecommunication costs<br>• Consistency with decentralized enterprise structure<br>• Business unit control over overhead costs | • Difficulty maintaining global standards and consistent data<br>• Higher infrastructure costs<br>• Difficulty negotiating preferential supplier agreements<br>• Loss of control<br>• Duplication of staff and data | VeriFone<br>FedEx[4] |

© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

---

## Figure 8.3 - Federal IT
The federal IT attempts to capture the benefits of centralized and decentralized organizations while eliminating the drawbacks of each
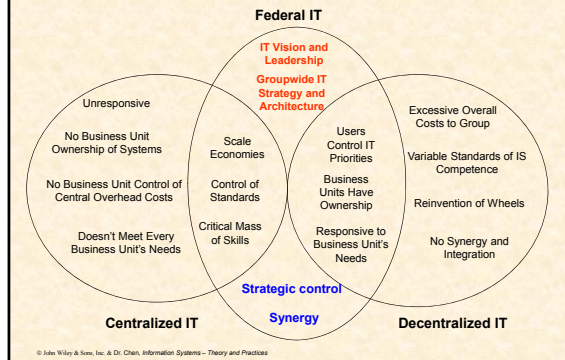


© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

---

## Another Perspective on IT Governance

- Peter Weill and his colleagues define *IT governance* as
  - *"specifying the __decision rights__ and __accountability__ framework to encourage desirable behavior in using IT."*
- IT governance is not about what decisions are actually made, but **who** :
  - *"Who is making the decisions (i.e., who holds the decision rights) and how the decision makers are held accountable for them."*
- Match the manager's decision rights with his or her accountability for a decision.
- Figure 8.4 indicates what happens when there is a *mismatch*.
- **Mismatches** result in either an oversupply of IT resources or the inability of IT to meet business demand.

© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

---

## Figure 8.4 IS decision rights-accountability gap – Indicates what happens when there is a mismatch.

| | | Accountability | |
|---|---|---|---|
| | | Low | High |
| Decision Rights | High | **Technocentric Gap**<br>• Danger of overspending on IT creating an oversupply<br>• IT assets may not be utilized to meet business demand<br>• Business group frustration with IT group | **Strategic Norm (Level 3 balance)**<br>Works where IT is viewed as competent and strategic to business |
| | Low | **Support Norm (Level 1 balance)**<br>Works for organizations where IT is viewed as a support function; focus is on business efficiency | **Business Gap**<br>• Cost considerations dominate IT decision<br>• IT assets may not utilize internal competencies to meet business demand<br>• IT group frustration with business group |

© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

---

## Figure 8.4 IS decision rights-accountability gap – Indicates what happens when there is a mismatch.

| | Accountability | | |
|---|---|---|---|
| | | **Low** | **High** |
| **Decision Rights** | **Low** | **Support Norm (Level 1 balance)**<br>Works for organizations where IT is viewed as a support function; focus is on **business efficiency** . | **Business Gap**<br>• __Cost__ considerations dominate IT decision<br>• IT assets may *not* utilize internal competencies to meet business demand<br>• IT group frustration with business group |
| | **High** | **Technocentric Gap**<br>• Danger of overspending on IT creating an oversupply.<br>• IT assets may *not* be utilized to meet business demand<br>• Business group frustration with IT group | **Strategic Norm (Level 3 balance)**<br>Works for organizations where IT is viewed as __competent__ and **strategic** to business. |

© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

---

## Another Perspective on IT Governance (Cont.)

- Good IT governance provides a *structure* to make good decisions.
- IT governance has two major components:
  - 1) The assignment of decision-making **authority** and __responsibility__ (Weill and Ross propose **archetypes** [a pattern for decision rights allocation] labeling the combinations of people who either *input* information or have decision rights for key IT *decisions* ; see Fig. 8.6)
  - 2) The decision-making **mechanisms** (e.g., policies, review boards, steering committees)
- Weill and his colleagues proposed *five* generally applicable categories of IT decisions:
  - 1) IT principles, 2) IT architecture, 3) IT infrastructure strategies, 4) business application needs, and 5) IT investment and prioritization.
  - Figure 8.5 provides a description of these decision categories with an example of major IS activities affected by them.

© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

## Another Perspective on IT Governance (Cont.-2)

- Good IT governance provides a structure to make good decisions.
- IT governance has two major components:
  - 1) The assignment of decision-making **authority** and **responsibility**
  - 2) The decision-making **mechanisms** (e.g., steering committees, review boards, policies).
- Weill and his colleagues proposed *five* generally applicable categories of IT decisions:
  - 1) IT principles, 2) IT architecture, 3) IT infrastructure strategies, 4) business application needs, and 5) IT investment and prioritization.
  - Figure 8.5 provides a description of these decision categories with an example of major IS activities affected by them.

---

**Figure 8.5 Five major categories of IT decisions.**

| Category | Description | Examples of Effected IS Activities |
|---|---|---|
| **IT Principles** | High-level statements about how IT is used in the business. | Participating in setting strategic direction. |
| **IT Architecture** | An integrated set of technical choices to guide the organization in satisfying business needs. The architecture is a set of policies and rules for the use of IT and plots a migration path to the way business will be done. | Establishing architecture and standards. |
| **IT Infrastructure Strategies** | Strategies for the base foundation of budgeted-for IT capability (both technical and human) shared throughout the firm as reliable services and centrally coordinated. | Managing Internet and network services, providing general support, managing data, managing human resources. |
| **Business Application Needs** | Specification of the business need for purchased or internally-developed IT applications. | Developing and maintaining IS. |
| **IT Investment & Prioritization** | Decision about how much and where to invest in IT, including project approvals and justification techniques. | Anticipating new technologies. |

---

## Political Archetypes

- Weill and Ross propose **archetypes** labeling the combinations of people who either *input* information or have decision rights for key IT *decisions* (i.e., *authority* and/or responsibility)
  - Business monarchy, IT monarchy, feudal, federal, IT duopoly, and anarchy.
- An *archetype* is a pattern for decision rights allocation.
- Decisions can be made at several levels in the organization (Figure 8.6).
  - Enterprise-wide, business unit, and region/group within a business unit.
- There is significant variation across organizations in terms of archetypes selected for decision right allocation.
  - The duopoly is used by the largest portion (36%) of organizations for IT principles decisions.
  - IT monarchy is the most popular for IT architecture (73%) and infrastructure decisions (59%).

---

**Figure 8.6 IT governance archetypes.**

| Decision rights or inputs rights for a particular IT decision are held by: | | CxO Level Execs | Corp. IT and/or Business Unit IT | Business Unit Leaders or Process Owners |
|---|---|---|---|---|
| **Business Monarchy** | A group of, or individual, business executives (i.e., CxOs). Includes committees comprised of senior business executives (may include CIO). Excludes IT executives acting independently. | ✓ | | |
| **IT Monarchy** | Individuals or groups of IT executives. | | ✓ | |
| **Feudal** | Business unit leaders, key process owners or their delegates. | | | ✓ |
| **Federal** | C level executives and at least one other business group (e.g., CxO and BU leaders)—IT executives may be an additional participant. Equivalent to a country and its states working together. | ✓ | ✓ | ✓ |
| | | ✓ | | ✓ |
| **IT Duopoly** | IT executives and one other group (e.g., CxO or BU leaders). | ✓ | ✓ | |
| | | | ✓ | ✓ |
| **Anarchy** | Each individual user. | | | |

© MIT Sloan Center for Information Systems Research 2003 - Weill

---

## IT Governance and Security

- Weill and Ross Framework for IT governance offers a new perspective for assigning responsibility for **key security decisions**.
- Figure 8.7 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.

---

**Figure 8.7 Matching information security decisions and archetypes.**

| Information Security Decision | Recommended Archetype | Rationale | Major Symptoms of Improper Decision Rights Allocation |
|---|---|---|---|
| Information Security Strategy | Business monarchy | Business leaders have the knowledge of the company's strategies, on which security strategy should be based. No detailed technical knowledge is required. | Security is an afterthought and patched on to processes and products. |
| Information Security Policies | IT duopoly | Technical and security implications of behaviors and processes need to be analyzed and trade-offs between security and productivity need to be made. Need to know the particularities of company's IT infrastructure. | Security policies are written based on theory and generic templates. They are unenforceable due to a misfit with the company's specific IT and users. |
| Information Security Infrastructure | IT monarchy | In-depth technical knowledge and expertise is needed. | There is a mis-specification of security and network typologies or a misconfiguration of infrastructure. Technical security control is ineffective. |
| 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. | Users are insufficiently trained, bypass security measures, or do not know how to react properly when security breaches occur. |
| 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. | Under- or over-investment in information security occurs. The human or technical security resources are insufficient or wasted. |

### Decision Making Mechanisms

- **Policies** are useful for the decision making process in certain situations.
- A review board or committee formally designated to *approve*, *monitor*, and *review* specific topics.
  - It can be an effective governance **mechanism**
- **IT steering committee**
  - an advisory committee of key stakeholders or experts can provide guidance on important IT issues.
  - Works well with federal archetypes, which call for joint participation of IT and business leaders.
- **IT Governance Council**
  - a steering committee at the highest level.
  - Reports to the board of the directors or the CEO.

---

### Governance Frameworks for Control Decisions

- Governance frameworks have been employed recently to define *responsibility* for **control** decisions.
- These frameworks focus on **processes** and **risks** associated with them.

---

### Traditional Technology vs. Consumerization of Technology

- *Traditional* IT organizations operated with a command and control mentality:
  - IT leaders made decisions about which technologies would be used.
- *Consumerization* of technology is a term used to describe the increasingly powerful tools available in the consumer **space** that are impacting the corporate space.
  - It covers cloud services, desktop application, *social networking*, devices, and the management policies surrounding them.
  - Its trend changed the management approach from "*How do we stop it*?" to "*How do we* **work** *with this*?"
  - Consumerization of IT is driven by employees who buy their own devices (*BYOD*), use their own personal online service accounts, install their own applications and then connect to the corporate network with the device, often without the organization's knowledge or approval.

---

# Sarbanes-Oxley Act of 2002

**WHAT**
**WHY**
**WHO**

---

### Sarbanes-Oxley Act of 2002: WHAT

- **What the term 'Sarbanes-Oxley' stands for**
  - Senator Paul *Sarbanes* and Representative Michael *Oxley*, who drafted the Sarbanes-Oxley Act of 2002.
- Also known as "*Public Company Accounting Reform and Investor Protection Act*"

---

### Sarbanes-Oxley Act of 2002: WHY

- The bill was enacted as a reaction to a number of major *corporate and accounting scandals* including those affecting *Enron*, Tyco International, Adelphia, and *WorldCom*.
  - These scandals, which cost investors billions of dollars when the share prices of affected companies collapsed, shook public confidence in the nation's *securities markets*.
- **The intent of the Sarbanes-Oxley Act**
  - To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

## Sarbanes-Oxley Act of 2002: WHO

- **Who the Act applies to**
  - SOX applies to all public companies in the U.S. and international companies that have registered equity or debt securities with the Securities and Exchange Commission (SEC) and the accounting firms that provide auditing services to them.

## Sarbanes-Oxley Act of 2002 (cont.)

- **What the Act is about**
  - The Sarbanes-Oxley Act created new standards for corporate accountability as well as new penalties for acts of wrongdoing.
  - It changes how corporate boards and executives must interact with each other and with corporate auditors. It removes the defense of "I *wasn't aware of* financial issues" from CEOs and CFOs, holding them accountable for the accuracy of financial statements.
  - The Act specifies new financial reporting responsibilities, including adherence to new internal controls and procedures designed to ensure the validity of their financial records.

## Sarbanes-Oxley Act of 2002 (cont.)

- **If a company isn't in compliance...**
  - What happens depends on which section of the act they're out of compliance with.
  - Non compliance penalties range from the loss of exchange listing, loss of D&O (Directors and Officers) insurance to multimillion dollar fines and imprisonment. It can result in a lack of investor confidence.
  - A CEO or CFO who submits a wrong certification is subject to a fine up to $1 million and imprisonment for up to ten years. If the wrong certification was submitted "willfully", the fine can be increased up to $5 million and the prison term can be increased up to twenty years.

## 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.

## IT and the Implementation of Sarbanes Oxley Act Compliance

- The most contentious aspect of SOX is Section 404, which requires management and the external auditor to report on the adequacy of the company's internal control on financial reporting (ICFR).
- CIO works with auditors, CFO, and CEO.
  - CIO must tread carefully
- 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 that focuses on aligning IT services with the needs of business.

## Sarbanes-Oxley Act of 2002 Summary

- 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 (stiff penalties).
  - 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.

## 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 corporations under the SEC are subject to SoX requirements.
  - Includes:
    - ✓U.S. and foreign companies that are traded on U.S. exchanges.
    - ✓companies that make up a significant part of a U.S. company's financial reporting.
- **CEOs** and **CFOs** must personally certify and be accountable for their firm's financial records and accounting.

---

## SoX - Financial Controls

- **Auditors** must certify the underlying controls and processes that are used to compile a company's financial results.
- Companies must provide real-time disclosures of any events that may affect a firm's stock price or financial performance within a **48**-hour period.
- Penalties for failing to comply range from fines to a 20-year jail term.
- **IT** plays a major role in ensuring the **accuracy** of financial data.

---

## SoX - IT Controls

Five IT control *weaknesses* are repeatedly uncovered by auditors:

1. *Failure* to segregate duties within applications as well as 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 ensure that systems were running smoothly and that there 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.

- IT managers must assess the level of controls needed to mitigate potential risks in organizational business processes.

---

## Frameworks for Implementing SoX

**COSO** (**C**ommittee **O**f **S**ponsoring **O**rganizations of the Treadway Commission)

and

**COBIT** (*Control **OB**jectives for **I**nformation and related **T**echnology*)

---

## Frameworks for Implementing SoX - COSO

- Treadway Commission (National Commission on Fraudulent Financial Reporting) was created as a result of financial scandals in the 1980s.
  - Members came from five highly esteemed accounting organizations.
  - These organizations became known as the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
- They created *three* **control objectives** for management and auditors that focused on dealing with **risks** to internal **control**:
  - **Operations** .
  - **Compliance** .
  - **Financial reporting.**
    - ✓ SoX is focused on this control objective.

---

## Frameworks for Implementing SoX – COSO

- Treadway Commission (National Commission on Fraudulent Financial Reporting) was created as a result of financial scandals in the 1980s.
  - Members came from five highly esteemed accounting organizations.
  - These organizations became known as the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
- They created *three* **control objectives** for management and auditors that focused on dealing with **risks** to internal **control**:
  - **Operations**.
  - **Compliance.**
  - **Financial reporting.**
    - ✓ SoX is focused on this control objective.

## COSO Business Framework

- COSO (**C**ommittee **O**f **S**ponsoring **O**rganizations of the Treadway Commission) established five essential **control** components for managers and auditors.
  1. Control environment—addresses the overall culture of the company.
  2. Risk assessment—most critical risks to internal controls.
  3. Control processes—outline important processes and guidelines.
  4. Information and communication of the procedures.
  5. Monitoring—by management of the internal controls.
- SoX:
  - requires public companies to define their **control framework**.
  - recommends COSO as the business framework for general accounting controls.
  - is not IT-specific.

## COBIT - Control Objectives for Information and Related Technology

- COBIT is an IT governance framework that is consistent with **COSO** controls that:
  - focus on making sure that IT provides the systematic rigor needed for SoX **compliance**.
  - provide a framework for linking IT processes, IT resources, and IT information to a company's strategies and objectives.
- Information Systems Audit & Control Association (ISACA) issued COBIT in 1996.
- COBIT provides a set of process goals, metrics, and practices (Figure 8.8).
  - Risk categorized into four major domains: planning and organization, acquisition and implementation, delivery and support, or monitoring.
  - The company determines the processes that are the most susceptible to the **risks** that it chooses to manage.

### Figure 8.8  Components of COBIT and their examples.

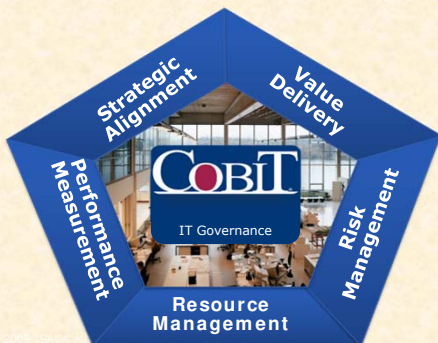| Component | Description | Example |
|---|---|---|
| Domain | One of four major areas of risk (plan and organize, acquire and implement, deliver and support, and monitor and evaluate); each domain consists of multiple processes | Delivery and support |
| Control Objective | Focuses on control of a process 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 preparation process and tasks" |
| Key Performance Indicator | Actual, highly specific measures 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 levels, 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 | "0—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" |

## COBIT – a Governance Framework

- The company identifies **processes** that it is going to manage.
- Sets up a **control** objective and more specific key goal indicators.
- *Advantages:*
  - Well-suited to organizations focused on risk management and mitigation.
  - designates clear ownership and responsibility for key processes in such a way that is understood by all organizational stakeholders.
  - COBIT provides a formal framework for **aligning** IS strategy with the business strategy.
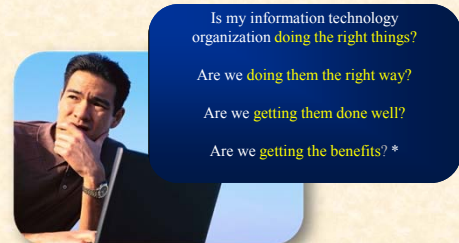- *Disadvantages:*
  - Very detailed.
  - Costly and time-consuming.

## Harmonizing the Elements of IT Governance

## COBIT® Answers Key Business Questions



Is my information technology organization doing the right things?

Are we doing them the right way?

Are we getting them done well?

Are we getting the benefits? *

*\* Based on the "Four Ares" as described by John Thorp in his book The Information Paradox, written jointly with Fujitsu, first published in 1998 and revised in 2003*

# The COBIT® Framework



© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

---
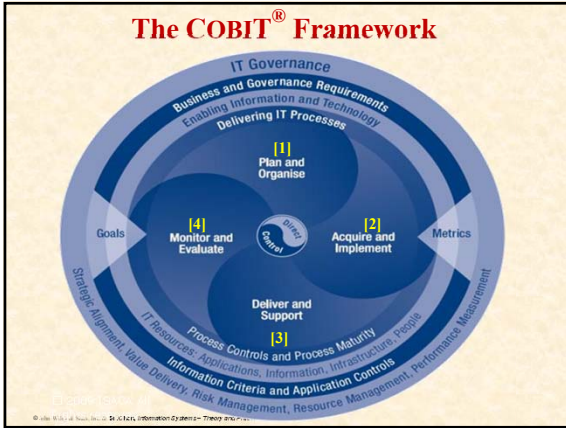
# COBIT® Defined Responsibilities for Each Process

## RACI Chart

A RACI chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

| Activities | CEO | CFO | Business Executive | CIO | Business Process Owner | Head Operations | Chief Architect | Head Development | Head IT Administration | PMO | Compliance, Audit, Risk and Security |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Link business goals to IT goals. | C | I | A/R | I | C | | | | | | |
| Identify critical dependencies and current performance. | C | C | R | A/R | C | C | C | C | C | | C |
| Build an IT strategic plan. | A | C | C | R | I | C | C | C | C | I | C |
| Build IT tactical plans. | C | I | | A | C | C | C | C | C | R | I |
| Analyse programme portfolios and manage project and service portfolios. | C | I | I | A | R | R | C | R | C | C | I |

© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

---

# Other Control Frameworks for SoX

- The International Standards Organization (ISO).
  - The world's largest developer and publisher of International Standards.
- Information Technology Infrastructure Library (ITIL).
  - A set of concepts and techniques for managing IT infrastructure, development, and operations.
  - Offers 8 sets of management procedures:
    - Service delivery, service support, service management, ICT infrastructure management, software asset management, business perspective, security management, and application management.
  - A widely **recognized** framework for IT service management and operations management that has been adopted around the globe.

© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

---

# IS and the Implementation of SoX Act Compliance

- The IS department and **CIO** are involved with the implementation of SoX.
- Section 404 deals with management's assessment of **internal controls**.
- Braganza and Franken provide six tactics that CIOs can use in working with auditors, CFOs, and CEOs (Figure 8.9):
  - Knowledge building.
  - Knowledge deployment.
  - Innovation directive.
  - Mobilization.
  - Standardization.
  - Subsidy.
- The extent to which a CIO could employ these various tactics depends upon the his/her power relating to the SoX implementation.

© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

---

**Figure 8.9 CIO Tactics for implementing SoX compliance.**



© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

---

# WHAT THE IS ORGANIZATION DOES NOT DO

© John Wiley & Sons, Inc. & Dr. Chen, *Information Systems – Theory and Practices*

## What IS Does Not Do

- Does not perform __*core*__ business functions such as:
  - Selling
  - Manufacturing
  - Accounting.
- Does not set __*business*__ strategy.
  - General managers must not delegate critical technology decisions.

## Categories of IT Governance (Decisions)

- Assume that you are CIO in your organization. When it comes specifically to IT governance, you and your colleagues propose six generally applicable categories of IT decisions. Which ONE of the following is **NOT** one of your categories?

- 1) IT cost and evaluation
- 2) IT principles
- 3) IT architecture
- 4) IT infrastructure strategies
- 5) Business application needs
- 6) IT investment and prioritization

## Management vs. Leader

- Management
  - Planning
  - Budgeting
  - Organizing
  - Staffing
  - Controlling
  - Problem-solving

- Leadership
  - Establishing direction
  - Aligning people
  - Motivating
  - Inspiring
  - Empowering
  - Problem-preventing

*"Soft"* **Interpersonal Skills**

- **Effective communication**
- **Deep listening**
- **Facilitating**
- **Negotiating**

- **Working with conflict**
- **Relationship building**
- **Understanding how to work effectively in teams**
- **Knowing when to say NO!**

## Conclusions

- The power of IS department now and the future will come from *leadership, influence* and *capability* - and less from *control*.
- The roadblock to competitive advantage generally is not technology, but *implementation* - with people.
- Alternative governance approaches are possible: centralized, decentralized and federalism (hybrid).
- A second governance approach involves decision rights
  - How to allocate decision rights in such a way as to encourage desirable behavior in the use of IT.
- A third governance approach is based on controls
  - Sarbanes-Oxley Act (2002) and
  - COBIT an IT governance framework based on control that can be used to promote IT-related internal controls and Sarbanes-Oxley compliance.