Managing and Using Information Systems: A Strategic Approach – Fifth Edition

Keri Pearlson and Carol Saunders

Chapter 8

Governance of the Information Systems Organization

PowerPoint® files by Michelle M. Ramim
Huizenga School of Business and Entrepreneurship
Nova Southeastern University

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**.

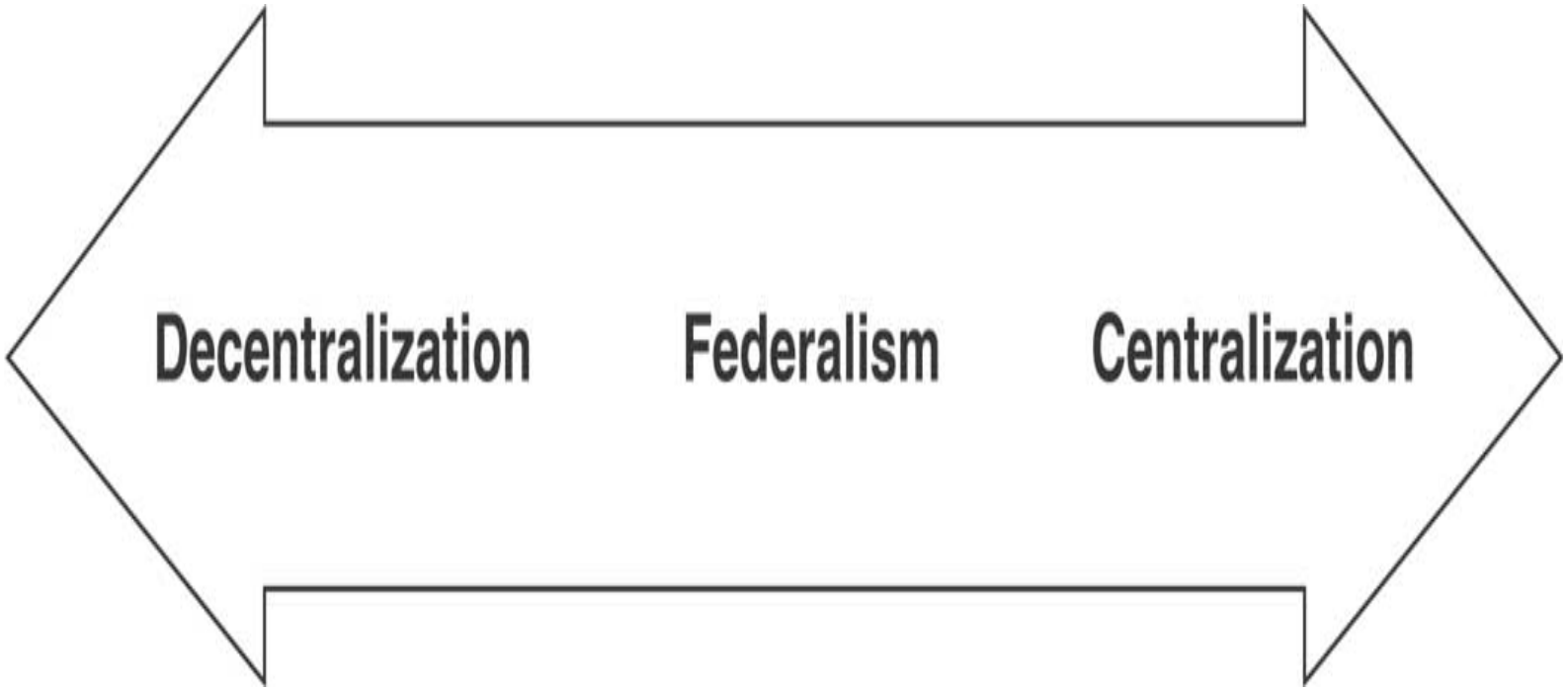
IT Governance

- **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 versus Decentralized Organizational Structures

- **Centralized** – brings together all staff, hardware, software, data, and processing into a single location.
- **Decentralized** – the components (e.g., staff, hardware, etc.) are scattered in different locations to address local business needs.
- **Federalism** – a combination of centralized and decentralized structures.
- Figure 8.1 shows the organizational structure continuum.
- Companies with higher levels of governance **maturity** have a need for control that is made possible in the centralized structure.

Figure 8.1 Organizational continuum.



Organizational Structural Approaches

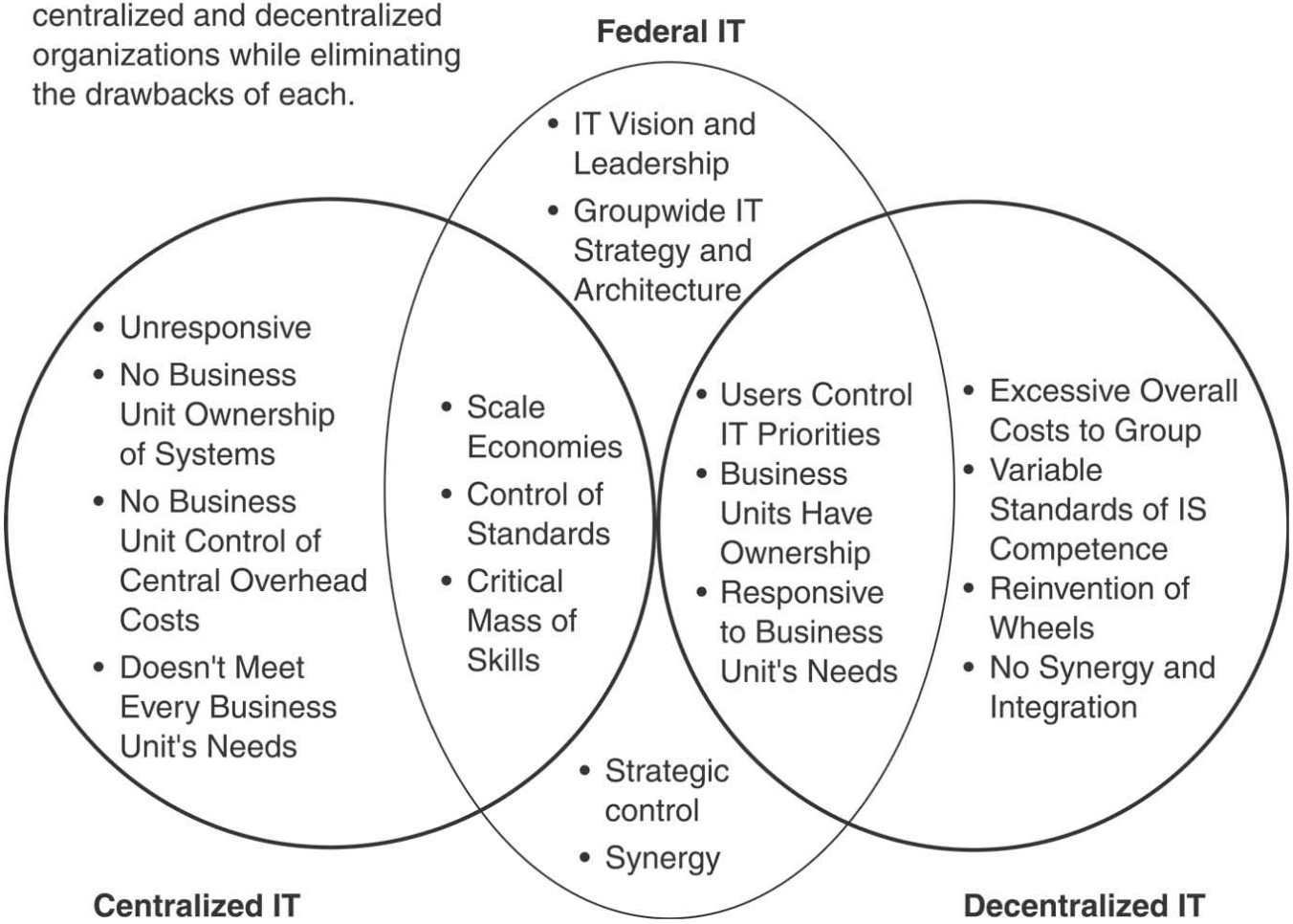
- Figure 8.2 shows advantages and disadvantages of each organizational approach.
- Most companies want to achieve the advantages derived from both organizational paradigms.
- **Federalism** is a structuring approach that distributes power, hardware, software, data, and personnel between a central IS 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 • "One voice" when negotiating supplier contracts • Greater leverage in deploying strategic IT initiatives • Economies of scale and a shared cost structure • Access to large capacity • Better recruitment and training of IT professionals • Better control of security and databases • Consistent with centralized enterprise structure	• Technology may not meet local needs • Slow support for strategic initiatives • Schism between business and IT organization • Us versus them mentality when technology problems occur • Lack of business unit control over overhead costs	Zara UPS[3]
Decentralized	• Technology customized to local business needs • Closer partnership between IT and business units • Greater flexibility • Reduced telecommunication costs • Consistency with decentralized enterprise structure • Business unit control over overhead costs	• Difficulty maintaining global standards and consistent data • Higher infrastructure costs • Difficulty negotiating preferential supplier agreements • Loss of control • Duplication of staff and data	VeriFone FedEx[4]

Figure 8.3 Federal IT.

The federal IT attempts to capture the benefits of centralized and decentralized organizations while eliminating the drawbacks of each.



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.
  - 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.

Figure 8.4 IS decision rights-accountability gap.

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

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**.
2. The decision-making mechanisms (e.g., steering committees, review boards, policies).

- Weill and his colleagues proposed five generally applicable categories of IT decisions:
  - IT principles, IT architecture, IT infrastructure strategies, business application needs, and 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.
  - 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—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.

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

- 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 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.

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.

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.

Figure 8.9 CIO Tactics for implementing SoX compliance.

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 requirements 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	Negotiating 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 overarching corporate compliance architecture
Subsidy	Funding implementers' 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

Chapter 8 - Key Terms

Archetype (p. 242) - a pattern from decision rights allocation.

Business continuity plan (BCP) (p. 250) - an approved set of preparations and sufficient procedures for responding to a variety of disaster events.

Centralized IS organizations (p. 238) - bring together all staff, hardware, software, data, and processing into a single location.

COBIT (Control Objectives for Information and Related Technology) (p. 253) - an IT governance framework that is consistent with COSO controls.

Chapter 8 - Key Terms (Cont.)

Decentralized IS organizations (p. 238) - scatter components in different locations to address local business needs.

Federalism (p. 240) - a structuring approach that distributes power, hardware, software, data, and personnel between a central IS group and IS in business units.

Governance (p. 237) - making decisions that define expectations, grant authority, or ensure performance.

IT governance (p. 241) - specifying the decision rights and accountability framework to encourage desirable behavior in using IT.

Chapter 8 - Key Terms (Cont.)

ITIL (Information Technology Infrastructure Library) (p. 255) - a set of concepts and techniques for managing IT infrastructure, development, and operations that was developed in the United Kingdom.

Review board (p. 249) - a committee formally designated to approve, monitor, and review specific topics; can be an effective governance mechanism.

Sarbanes–Oxley Act (SoX) (p. 251) - enacted in the U.S. in 2002 to increase regulatory visibility and accountability of public companies and their financial health.

Steering committee (p. 249) - an advisory committee of key stakeholders or experts that provides guidance on important IT issues.

Copyright 2013 John Wiley & Sons, Inc.