chapter 9

Governance of the Information Systems Organization

Governance structures define the way decisions are made in an organization. This chapter explores four models of governance based on the location of decision making in organization structure (centralized, decentralized, and federal), decision rights, digital ecosystems, and control, considering frameworks from the Committee of Sponsoring Organizations of the Treadway Commission (COSO), Control Objectives for Information and related Technology (COBIT), and Information Technology Infrastructure Library (ITIL). Examples and strategies for implementation are discussed.

Intel's information technology (IT) performance reports for 2013[1] and 2015[2] boast about how the company increased its storage capacity from 25 petabytes in 2010 to 106 petabytes in 2014, and over the same interval raised the number of handheld devices from 19,400 to 53,700. Intel also exploited other highly visible opportunities of using predictive data analytics. It reduced the amount of time required to detect data threats from two weeks in 2013 to 20 minutes in 2014. Finally, Intel enjoyed a revenue increase of $351 million from advanced analytics in the areas of sales leads, supply, demand, and pricing.

An outsider might assume that Intel stepped up spending and IT investments to accomplish these goals. However, it actually *reduced* the number of data centers from 91 in 2010 to 61 in 2014 and reduced IT spending from 2.64% to 2.30% of revenue during that same five-year interval.

How did Intel accomplish these and other laudable goals? Its approach was the result of 23 years of evolution of its strategy that began by creating a centralized IT organization in 1992 with control resting in IT. Intel has come a long way from its original governance structure, which was centered on mainframes and wide-area networks. Later, in 2003, Intel initiated its "Protect Era" in response to two events: the then-new Sarbanes–Oxley legislation and a virus that had infected Intel's internal networks through an employee's home-based network connection. The company's "Protect Era" was led by IT and locked down resources to such an extent that employees had to devise risky policy workarounds to be able to complete some of their tasks. Data could be used only within a particular functional area, not shared among areas.

Intel's current "Protect to Enable Era" in information governance began in 2009 after managers found that its overly restrictive policies on bring your own device (BYOD) had frustrated its employees who saw those policies as both expensive and detrimental to innovation over the long run. This led Intel to discover that **consumerization** is a powerful force. That six-syllable mouthful describes the increasingly powerful tools available in the consumer space that can impact the corporate space. Mobility has been the major breakthrough in consumerization, and the increasing use of

[1] http://www.intel.com/content/dam/www/public/us/en/documents/reports/2012-2013-intel-it-performance-report.pdf (accessed September 1, 2015).
[2] http://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/intel-it-annual-performance-report-2014-15-paper.html (accessed September 1, 2015).

smartphones, tablets, and smaller/more powerful laptops coupled with Web-based applications that offer everything from free business productivity tools, such as Google Docs to sharing applications like YouTube and SlideShare and to social tools such as Twitter and LinkedIn, have created a new IT environment.

Intel found that cloud services, desktop applications, social networking, mobile devices, and the management policies surrounding them had changed the business of IT. BYOD forced IT leaders at Intel and many other firms to re-evaluate how IT services are offered. Intel's traditional command and control mentality—with IT leaders making all technology decisions—no longer could work. The consumerization of technology changed Intel's management approach[3] from "How do we stop it?" to "How do we work with this?"

Intel's governance structure also resulted in a lost opportunity to exploit data and analytics (described in Chapter 13). Because information was restricted to the particular department in which it was generated, Intel could not explore connections between manufacturing decisions and consumer reactions or between social media trends and product design decisions. A new approach to governance was clearly needed, and Protect to Enable has addressed those needs.

More recently, Intel has extended the governance framework's reach by its new six-pronged focus on social networking, mobile devices, analytics, cloud technologies, Internet of Things, and security. Intel reports that it has now moved to the top of a three-tiered pyramid of IT leadership of (1) developing programs and delivering services, (2) contributing business value, and (3) transforming the company.

How does a governance framework provide these benefits? Intel now uses information governance boards that include representatives from a variety of its functions, including marketing, manufacturing, product design, human resources (HR), legal, business development, internal audit, and IT. Sharing the governance with business units is one of five key success factors, according to an analysis of the Intel case.[4] Intel reports that they have moved beyond categorizing challenges as IT problems or business problems. They assert that only integrated solutions work to "disrupt instead of being disrupted."[5]

Although each information systems (IS) organization is unique in many ways, all have elements in common. The focus of this chapter is to introduce managers to issues related to the way decisions about IT are made in the organization. These issues should reflect the typical activities of an IS organization that were discussed in Chapter 8. The current chapter examines governance of the IS organization as it relates to decisions about IT issues.

IT Governance

Expectations (or more specifically, what managers should and should not expect from the IS organization) are at the heart of IT governance. **Governance** in the context of business enterprises is all about making decisions that define expectations, grant authority, or ensure performance. In other words, governance is about aligning behavior with business goals through empowerment and monitoring. Empowerment comes from granting the right to make decisions, and monitoring comes from evaluating performance. As noted in Chapter 3, a decision right is an important organizational design variable because it indicates who in the organization has the responsibility to initiate, supply information for, approve, implement, and control various types of decisions.

Four perspectives of IT governance are described here. The first, a traditional perspective of IT governance, focuses on how decision rights can be distributed to facilitate centralized, decentralized, or hybrid modes of decision making. In this view of governance, the organization structure plays a major role. The second focuses on the interaction between accountability and allocation of decision rights to executives, business unit leaders, or IT leaders. The third focuses on an "ecosystem" that reflects the significant impacts of the large variety of resources available from individuals, organizational units, and outside service providers. The final perspective, control structures developed in response to important legislation, also provides governance guidelines to firms.

---

[3] Paul P. Tallon, James E. Short, and Malcolm Harkins, "The Evolution of Information Governance at Intel," *MIS Quarterly Executive* 12, no. 4 (2013), 189–98.

[4] Ibid.

[5] http://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/intel-it-annual-performance-report-2014-15-paper.html, 20 (accessed September 3, 2015).

Centralized versus Decentralized Organizational Structures

Companies' organizational strategies exist along a continuum from centralization to decentralization. At one end of the continuum, **centralized IS organizations** bring together all staff, hardware, software, data, and processing into a single location. **Decentralized IS organizations** scatter these components across different locations to address local business needs. These two approaches do not refer to IT architectures but to decision-making frameworks. A combination, or hybrid, of the two is called *federalism*, found in the middle (see Figure 9.1). Enterprises of all shapes and sizes can be found at any point along the continuum. Over time, however, each enterprise may gravitate toward one end of the continuum or the other, and often reorganization is in reality a change toward one end to the other.

Centralization and decentralization trends have evolved through the five eras of information usage (see Chapter 2, Figure 2.1). In the 1960s, mainframes dictated a centralized approach to IS because the mainframe resided in one physical location. Centralized decision making, purchasing, maintenance, and staff kept these early computing behemoths running. The 1970s remained centralized due in part to the constraints of mainframe computing, although minicomputers planted early seeds for decentralizing. In the 1980s the advent of the personal computer (PC), which allowed computing power to spread beyond the raised-floor, super-cooled rooms of mainframes, provided further fuel for decentralization. Users especially liked the shift to decentralization because it put them more in control and increased their agility. However, the pressures for secure networks and massive corporate databases in the 1990s shifted some organizations back to a more centralized approach. Yet, the increasingly global nature of many businesses makes complete centralization impossible. The most recent global survey found that 70.6% of the participating organizations were centralized in terms of IT, 13.5% were decentralized, and 12.7% were federated.[6] Although the high percentage of centralized companies in the sample may seem surprising, the study suggested that with the increasing appreciation for governance found in companies with high levels of governance maturity comes the need for control that is made possible in the centralized structure.

The survey also found that two-thirds of responding enterprises had governance activities for enterprise IT (GEIT). These companies indicated that the main driver for GEIT activities is to ensure that IT functionality aligns with business needs, and, like Intel's findings, the most commonly experienced outcomes were improvements in management of IT-related risk and communication and relationships between business and IT. Good governance therefore can increase the transparency of IT supply and demand and help in assigning priorities for IT projects and services.

What are the most important considerations in deciding how much to centralize or decentralize? Figure 9.2 shows some advantages and disadvantages of each approach.

Consider two competing parcel delivery companies, UPS and FedEx, in the year that they both reported spending about $1 billion on IT. UPS's IT strategy focused on delivering efficiencies to meet the business demands of consistency and reliability. UPS's centralized, standardized IT environment supported dependable customer service at a relatively low price. In contrast, FedEx chose a decentralized IT strategy that allowed it to focus on flexibility in meeting business demands generated from targeting various customer segments. The higher costs of the decentralized approach to IT management were offset by the benefits of localized innovation and customer responsiveness.[7]

FIGURE 9.1 Organizational continuum.

[6] IT Governance Institute, "Global Status Report on the Governance of Enterprise IT (GEIT)" (2011), 49, http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-10Jan2011-Research.pdf (accessed February 27, 2011).

[7] J. W. Ross and P. Weill, "Six IT Decisions Your IT People Shouldn't Make," *Harvard Business Review* (November 2002), 1–8.

Approach	Advantages	Disadvantages	Companies Adopting
Centralized	• Global standards; common data • "One voice" for negotiating supplier contracts • Greater leverage in deploying strategic IT initiatives • Economies of scale and a shared cost structure • Access to large capacity • Improved recruitment and training of IT professionals • Improved 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[a]
Decentralized	• Technology customized to local business needs • Close partnership between IT and business units • Greater flexibility • Reduced telecommunication costs • Consistency with decentralized enterprise structure • Business unit control of overhead costs	• Difficulty in maintaining global standards and consistent data • Higher infrastructure costs • Difficulty in negotiating preferential supplier agreements • Loss of control • Duplication of staff and data	VeriFone, FedEx[b]

[a] J. W. Ross and P. Weill, "Six IT Decisions Your IT People Shouldn't Make," *Harvard Business Review* (November 2002), 1–8.
[b] Ibid.

FIGURE 9.2 Advantages and disadvantages of organizational approaches.

Zara, the global retail and apparel manufacturer introduced in Chapter 2, also used a centralized approach, which differs from other clothing chains. The head of IS, who was not a CIO, reported directly to the deputy general manager, who was two levels below the CEO.[8] This way of structuring the IS department was consistent with the organization's predominantly centralized structure. It was also well suited to organizational processing about which most administrative decisions were made in the headquarters at Lacoruña, Spain. The users did not require a lot of hand-holding with regard to the point-of-sale (POS) systems in the stores. For these reasons, a centralized approach was a good fit for Zara. The store managers, however, did retain some decision rights about which products to order. Thus, Zara was not totally at the centralization end of the continuum. In contrast, Verifone, which we discuss in Chapter 4, needs a decentralized structure for its globally distributed employees.

Companies adopt a strategy based on lessons learned from earlier years of centralization and decentralization. Most companies want to achieve the advantages derived from both organizational paradigms. This desire leads to **federalism**,[9] a structuring approach that distributes power, hardware, software, data, and personnel between a central IS group and IS in business units. Many companies adopt a form of federal IT yet still count themselves as either decentralized or centralized, depending on their position on the continuum. Organizations such as Home Depot and the U.S. Department of Veteran Affairs recognize the advantages of a more hybrid approach and actively seek to benefit from adopting a federal structure. See Figure 9.3 for the interrelationship of these approaches.

Archetypes of Accountability and Decision Rights

Sometimes the centralized/decentralized/federal approaches to governance are not fine-tuned enough to help managers deal with the many contingencies facing today's organizations. This issue is addressed by a framework

[8] Andrew McAfee, Vincent Dessain, and Anders Sjman, "Zara: IT for Fast Fashion," Harvard Business School Case 9-604-081 (September 6, 2007).
[9] John F. Rockart, Michael J. Earl, and Jeanne W. Ross, "Eight Imperatives for the New IT Organization," *Sloan Management Review* (Fall 1996), 52–53.

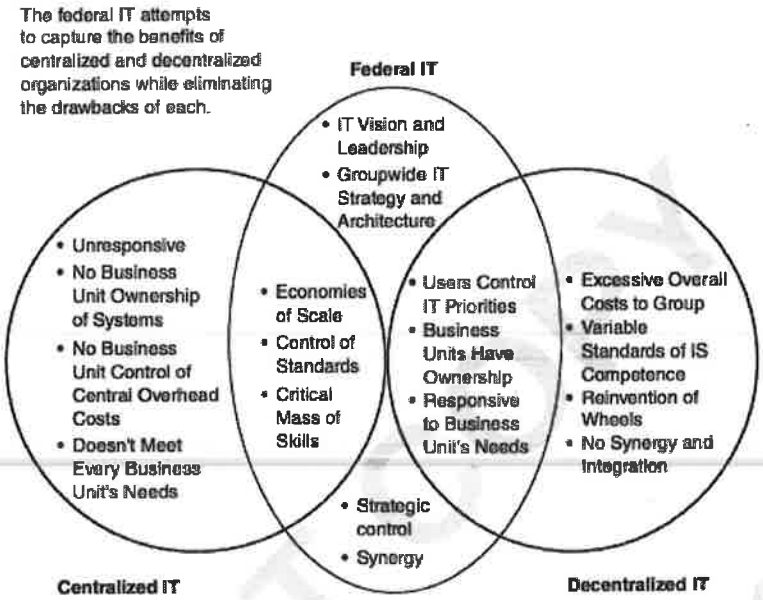

FIGURE 9.3 Federal IT.
Source: Michael J. Earl, "Information Management: The Organizational Dimension," *The Role of the Corporate IT Function in the Federal IT Organization*, ed. S. L. Hodgkinson (New York: Oxford University Press, 1996), Figure 12.1. By permission of Oxford University Press, Inc.

developed by Peter Weill and Jeanne Ross. They define **IT governance** as "specifying the decision rights and accountability framework to encourage desirable behavior in using IT."[10] IT governance is not about what decisions are actually made but rather about who is making them (i.e., who holds the decision rights) and how the decision makers are held accountable for them.

It is important to match the manager's decision rights with his or her accountability for a decision. Figure 9.4 indicates what happens when there is a mismatch. Where the CIO has a high level of decision rights and accountability, the firm is likely to be at maturity Level 3 (which was introduced in Chapter 8). Where both the decision rights and accountability are low, the company is likely to be at Level 1. Mismatches result in either an oversupply of IT resources or the inability of IT to meet business demand.

Good IT governance provides a structure to make good decisions. It can also limit the negative impact of organizational politics in IT-related decisions. IT governance has two major components: (1) assignment of decision-making authority and responsibility and (2) decision-making mechanisms (e.g., steering committees, review boards, policies). When it comes specifically to IT governance, 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.[11] A description of these decision categories with an example of major IS activities affected by them is provided in Figure 9.5.

Weill and Ross's study of 256 enterprises shows that a defining trait of high-performing companies is the use of proper decision right allocation patterns for each of the five major categories of IT decisions. They use six political archetypes with highly descriptive names (business monarchy, IT monarchy, feudal, federal, IT duopoly, and anarchy) to label the combinations of people who either input information or have decision rights for the key

[10] Peter Weill and Jeanne W. Ross, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results* (Cambridge, MA: Harvard Business School Press, 2004); Peter Weill, "Don't Just Lead, Govern: How Top-Performing Firms Govern IT," *MIS Quarterly Executive* 3, no. 1 (2004), 1–17. The quote is on page 3.

[11] P. Weill, "Don't Just Lead, Govern: How Top-Performing Firms Govern IT," *MIS Quarterly Executive* 3, no. 1 (2004).

		Accountability	
		Low	High
Decision Rights	High	**Technocentric gap** • There is danger of overspending on IT, creating an oversupply • IT assets may not be utilized to meet business demand • Business group might become frustrated with IT group	**Strategic norm (Level 3 balance)** • IT is viewed as competent • IT is viewed as strategic to business
	Low	**Support norm (Level 1 balance)** • It works for organizations where IT is viewed as a support function • Its 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 might cause frustration for business group

FIGURE 9.4 IS Decision rights accountability gap.
Source: Adapted from V. Grover, R. M. Henry, and J. B. Thatcher, "Fix IT-Business Relationships through Better Decision Rights," *Communications of the ACM* 50, no. 12 (December 2007), 82, Figure 1.

Category	Description	Examples of Affected IS Activities
IT principles	How to determine IT assets that are needed	Participating in setting strategic direction
IT architecture	How to structure IT assets	Establishing architecture and standards
IT infrastructure strategies	How to build IT assets	Managing Internet and network services, data, human resources, mobile computing
Business application needs	How to acquire, implement, and maintain IT (insource or outsource)	Developing and maintaining information systems
IT investment and prioritization	How much to invest and where to invest in IT assets	Anticipating new technologies

FIGURE 9.5 Five major categories of IT decisions.
Source: Adapted from P. Weill, "Don't Just Lead, Govern: How Top-Performing Firms Govern IT," *MIS Quarterly Executive* 3, no. 1 (2004), 4, Figure 2.

IT decisions.[12] An **archetype** is a pattern resulting from allocation of decision rights. Decisions can be made at several levels in the organization: top executives, IT executives, or business unit executives. Figure 9.6 summarizes the level and function for the allocation of decision rights in each archetype.

For each decision category, the organization adopts an archetype as the means to obtain inputs for decisions and to assign accountability for them. Although there is little variation in the selection of archetypes regarding who provides information for decision making, there is significant variation across organizations in terms of archetypes selected for decision right allocation. For instance, the duopoly is used by the largest portion (36%) of organizations for IT principles decisions whereas the IT monarchy is the most popular for IT architecture and infrastructure decisions (i.e., 73% and 59%, respectively).[13]

There is no one best arrangement for the allocation of decision rights. Rather, the most appropriate arrangement depends on a number of factors, including the type of performance indicator. Some common performance indicators are asset utilization, profit, or growth.

[12] Peter Weill and Jeanne W. Ross, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results* (Cambridge, MA: Harvard Business School Press, 2004).
[13] Weill and Ross, *IT Governance*.

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.			

FIGURE 9.6 IT governance archetypes.
Source: P. Weill, "Don't Just Lead, Govern: How Top-Performing Firms Govern IT," *MIS Quarterly Executive* 3, no. 1 (2004), 5, Figure 3.

Emergent Governance—The Digital Ecosystem

New consumer technologies challenge a "top-down" governance approach for making all decisions in a planned and methodical manner. The best-laid plans are often derailed. Intel's decree to lock down data and strictly control devices used by employees grew so difficult that it impeded the company's ability to not only compete but also to fulfill everyday tasks. Sometimes the best plans aren't even prescribed far in advance; in some situations, they simply emerge. For instance, social networking was ignored by many firms in its early days because they failed to recognize its impact. Most firms now realize that social networking needs not only recognition but also strategic investments.

There are many freely available and widely used apps, Web sites, social networks, smartphones, and other IT assets; it would be foolish to try to invent something identical in house, so firms often exploit them. Using a variety of such assets implies that governance might need to be more flexible and follow patterns of adaptation much like biological ecosystems, forming an interrelated set of interacting species.[14] Just as a species cannot ignore predators, prey, and complementary species, an information systems department cannot ignore new technologies and information assets that emerge suddenly and unexpectedly. One interesting definition of **digital ecosystem** regards those systems as self-interested, self-organizing, and autonomous digital entities.[15]

A simple example can be useful. Before YouTube, firms had to find their own way to provide digital video content to customers on the Web. Some used animations that were available in special image formats whereas others had to choose between requiring a download of a video file that they hoped would be playable on a user's computer or streaming a file to users who had to also install a particular streaming player that was compatible with the streaming video. Providing that content widely was not generally considered to be feasible or even desirable. With YouTube, firms can now simply use a link or even embed the video into their own Web site. Coupling this

[14] Maja Hadzic and Elizabeth Chang, "Application of Digital Ecosystem Design Methodology within the Health Domain," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans* 40, no. 4 (2010): 779–88.
[15] Rahnuma Kazi and Ralph Deters, "Mobile Event-Oriented Digital Ecosystem," *Digital Ecosystems Technologies (DEST), 2012 6th IEEE International Conference* (2012).

new simplicity with an ability to display a map from Google Maps forms new and very useful interdependencies between these digital assets.

In recent years, mobile computing, GPS, and social media have indeed presented new, unexpected challenges and opportunities as described earlier. However, other technological developments have also provided digital ecosystem opportunities, such as cloud computing, the Internet of Things (IoT), radio frequency ID (RFID), and smart cards. Interconnecting firms with each other allows connectivity in new, unpredictable, and very helpful ways.

A good example in the health care arena is an electronic medical record (EMR).[16] An EMR is filled with a variety of information about a patient (for instance, patient demographics, appointments, medications, medical history, billing records). Not only can a doctor's computer pick out the relevant information about a patient to use but also a pharmacy can identify potential drug interactions and a laboratory can be informed of certain medical conditions when processing a specimen. In addition, both the pharmacy process and the insurance company can bill for the medication and the appointment.

Some or all of these functions could have been in the original plans for EMRs, but others might occur to enterprising designers along the way. For instance, a bank that is administering the patient's flexible spending account can be provided medical billing information for properly disbursing funds. Also, a tax authority might be provided billing information from the EMR to verify deductible expenses. Each party would be privy only to the relevant information for it, and the rest would be kept confidential.

A smartphone provides another example of how a digital ecosystem can form between applications, firms, and digital entities. Even just the junction of identity, date, location, preference, and relationship information can provide real-time driving directions, invitations to nearby events, alerts about nearby friends, personalized advertising, and chatter on social network alerts. Many of these uses were not even imagined 15 years ago, and it is hard to imagine the possible new connections and uses that will occur in another 15 years. For instance, new ecosystem connections will be made possible when the IoT places more technology into automobiles. A self-driving car could actually react independently to an urgent situation with a family member and safely make a split-second decision to change course before all of the information is fully comprehended by the occupant (formerly called the "driver"). Individual devices and applications that are difficult to imagine today might be combined in new ways on the road, in the home, and at the office.

Strong governance implications emerge from ecosystems. The symbiotic multifirm and adaptive situations cannot be completely planned or orchestrated by a single entity. Much of the decision making exists outside the firm, and, therefore, complete plans no longer can be made in a single boardroom. Along with the good news of synergies between with and among various "apps" and devices, there is the potential danger of changes to the information passed between them or even the complete failure of an outside entity. Imagine what hotels would need to do if Google Maps would disappear altogether. Further, what would need to be done with location-based ads if predictions come true that one or more of the GPS satellites would fail[17] and are also vulnerable to attack?[18]

Fortunately, most ecosystems have adopted stringent standards for data exchange, and the most useful ones are quite successful. The likelihood of a permanent failure of Google Maps is quite remote for the foreseeable future. Even if Google were to divest the app, a new firm would likely be able to maintain the tightly specified connections. IT governance is perhaps most vulnerable to an inability to imagine strategic potential from new devices, applications, and connections. A firm should explore whether plans can be changed in mid-year. Can competitors become allies? Can business processes be changed quickly? Can new capabilities that might be contrary to previous activities or directions be enabled? Firms in the future will probably need to answer all of these questions in the affirmative for their ultimate survival.

To summarize the three governance frameworks, see Figure 9.7 for the main concept and potential best practice of each framework.

---

[16] Hadzic and Chang, "Application of Digital Ecosystem Design Methodology within the Health Domain."

[17] "GPS System Close to Breakdown," http://www.theguardian.com/technology/2009/may/19/gps-close-to-breakdown (accessed September 4, 2015).

[18] "Global Positioning System Is a Single Point of Failure," http://www.afcea.org/content/?q=global-positioning-system%E2%80%A8-single-point-failure (accessed September 4, 2015).

Governance Framework	Main Concept	Possible Best Practice
Centralization-Decentralization	Decisions can be made by a central authority or by autonomous individuals or groups in an organization.	Use a hybrid, federal approach.
Decision archetypes	Patterns based upon allocating decision rights and accountability are specified.	Tailor the archetype to the situation.
Digital ecosystems	Members of the ecosystem contribute their strengths, giving the whole ecosystem a complete set of capabilities that can impact decision making and operations.	Build flexibility and adaptability into governance.

FIGURE 9.7 Three governance frameworks.

Decision-Making Mechanisms

Many different types of mechanisms can be created to ensure good IT governance. Policies are useful for defining the process of making a decision under certain situations. However, when the environment is complex, policies are often too rigid. In a recent worldwide study of IT governance, almost 60% of the respondents relied on policies and standards for governance, making it the most popular mechanism for governance.[19] A second method, a **review board**, or committee that is formally designated to approve, monitor, and review specific topics, can be an effective governance mechanism. For example, Twila Day, CIO of Sysco, established an architecture review board to look at new technologies and processes.[20]

A third mechanism that is used very frequently for IT decisions is the IT **steering committee**, also called an IT *governance council*. Such a committee is composed of key stakeholders or experts who provide guidance on important IT issues. Steering committees work especially well with the federal archetype, which calls for joint participation of IT and business leaders in the decision-making process. Steering committees can be geared toward different levels of decision making. The highest level of steering committees report to the board of directors or the CEO and are often composed of top-level executives and the CIO. At this level, the steering committee provides strategic direction and funding authority for major IT projects and ensures that adequate resources be allocated to the IS organization for achieving strategic goals.

Committees with lower-level players typically are involved with allocating scarce resources effectively and efficiently. Lower-level steering committees provide a forum for business leaders to present their IT needs and to offer input and direction about the support they receive from IT operations.

Either level may have working groups to help increase the steering committee's effectiveness and to measure the performance of the IS organization. The assessment of performance differs for each group. For example, the lower-level committee likely would include more details and would focus on the progress of the various projects and adherence to the budget. The higher-level committee would focus on the performance of the CIO and the ability of the IS organization to contribute to the company's achievement of its strategic goals.

Although an organization may have both levels of steering committees, it is more likely to have one or the other. If the IS organization is viewed as being critical for the organization to achieve its strategic goals, the firm's C-level executives are likely to be on the committee. Otherwise, the steering committee tends to be larger so that it can have widespread representation from the various business units. In this case, the steering committee is an excellent mechanism for helping the business units realize the competing benefits of proposed IT projects and develop an approach for allocating among the project requests.

[19] IT Governance Institute, "Global Status Report on the Governance of Enterprise IT (GEIT)" (2011), 49, http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-10Jan2011-Research.pdf (accessed February 27, 2011).

[20] Martha Heller, "*How to Make Time for Strategy*," CIO.com (April 22, 2010), http://www.cio.com/article/591719/How_to_Make_Time_for_Strategy (accessed January 16, 2012).

For example, when Hilton Worldwide's CIO started working on a project to create a new loyalty program, he and the business sponsor of the project convened a lower-level steering committee made up of people from IT, marketing, HR, finance, and other departments. They discussed change management and business issues that arose as they designed the system to be used in 85 countries in over ten brands in the Hilton portfolio. The project went very smoothly. But earlier, another project to outsource the hotel help desk had not gone as well. The CIO learned from both experiences that there is no such thing as too much communication and created weekly steering committee meetings for each project. The CIO is quoted as saying, "E-mail is great for scheduling meetings, but it's the steering committees where we are working through really difficult issues together, and making promises and keeping promises, where the foundations of trust are established."[21]

Governance Frameworks for Control Decisions

The framework described previously focuses on which department is responsible for decisions. More recently, governance frameworks have been employed specifically to define responsibility for control decisions. They are being implemented to help ward off future accounting fiascos. These frameworks focus on processes and risks associated with them.

Sarbanes–Oxley Act of 2002

In response to rogue accounting activity by major global corporations such as Enron and WorldCom and their accounting firms, such as Arthur Andersen, the **Sarbanes–Oxley Act (SoX)** was enacted in the United States in 2002 to increase regulatory visibility and accountability of public companies and their financial health. The U.S. government wanted to assure the investing public that they could rely on financial markets to deliver valid performance data and accurate stock valuation. All corporations that fall under the jurisdiction of the U.S. Securities and Exchange Commission are subject to SoX requirements. This includes not only U.S. and foreign companies that are traded on U.S. exchanges but also those entities that make up a significant part of a U.S. company's financial reporting. Within five years of SoX's passage, 15,000 U.S. companies, 1,200 non-U.S.-based companies, and over 1,400 accounting firms in 76 countries have been affected by SoX.[22]

According to SoX, CFOs and CEOs must personally certify and be accountable for their firms' financial records and accounting (Section 302), auditors must certify the underlying controls and processes that are used to compile the financial results of a company (Section 404), and companies must provide real-time disclosures of any events that may affect their stock price or financial performance within a 48-hour period (Section 409). Penalties for failing to comply range from monetary fines to a 20-year jail term.

A comprehensive Public Company Accounting Oversight Board (PCAOB) review of 2,800 engagements of the largest audit firms found hundreds of cases involving audit failures, suggesting that improvements could be made in audit firm performance as well as the PCAOB's process for assessing and reporting on engagements. However, the review reported that SoX has been successful in increasing corporate focus on a strong ethical culture in publicly owned companies.[23]

Although SoX was not originally aimed at IT departments, it soon became clear that IT played a major role in raising the accuracy of financial data. Consequently, in 2004 and 2005, there was a flurry of activity as IT managers

---

[21] Adapted from "Candid Talk Trumps the Blame Game," CIO.com (November 2011), http://www.cio.com/article/693018/Candid_Talk_Trumps_the_Blame_Game (accessed September 4, 2015); "How CIOs Build Bridges with Other C-Level Execs," CIO.com (November 2011), http://www.cio.com/article/2402725/relationship-building-networking/how-cios-build-bridges-with-other-c-level-execs.html (accessed September 4, 2015).

[22] These figures were derived from the Public Company Accounting Oversight Board (PCAOB) as reported in Ashley Braganza and Arnoud Franken, "SoX, Compliance, and Power Relationships," *Communications of the ACM* 50, no. 9 (September 2007), 97–102.

[23] Curtis Verschoor, "Has SoX Been Successful," September 5, 2012, http://www.accountingweb.com/article/has-sox-been-successful/219796 (accessed March 27, 2015).

identified controls, determined design effectiveness, and validated operational controls through testing. Five IT control weaknesses repeatedly were uncovered by auditors:[25]

1. Failure to segregate duties within applications, 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 are running smoothly and that there is an audit of the audit log.
4. Failure to identify abnormal transactions in a timely manner.
5. Lack of understanding of key system configurations.

Although SoX's focus is on financial controls, many auditors encouraged (forced) IT managers to extend their focus to organizational controls and risks in business processes. This means that IT managers must assess the level of controls needed to mitigate potential risks in organizational business processes. As companies move beyond SoX certification into maintaining compliance, IT managers must be involved in ongoing and consistent risk identification, actively recognize and monitor changes to the IS organization and environment that may affect SoX compliance, and continuously improve IS process maturity. It is likely that managers will turn to software to automate many of the needed controls.

Frameworks for Implementing SoX

COSO

The Enron and WorldCom major financial scandals were not the first. In the wake of financial scandals in the mid-1980s, the Treadway Commission (or National Commission on Fraudulent Financial Reporting) was created. Its head, James Treadway, had previously served as commissioner of the SEC. The members of the Treadway Commission came from five highly esteemed accounting organizations: Financial Executives International (FEI), American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Institute of Internal Auditors (IIA), and Institute of Management Accountants (IMA). These organizations became known as the *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*. The commission created three control objectives for management and auditors that focused on addressing risks to internal control. These control objectives deal with:

- *Operations:* To help the company maintain and improve its operating effectiveness and protect the assets of shareholders
- *Compliance:* To ensure that the company is in compliance with relevant laws and regulations
- *Financial reporting:* To ensure that the company's financial statements are produced in accordance with generally accepted accounting principles (GAAP). *SoX is focused on this control objective.*

To make sure a company meets its control objectives, COSO established five essential control components for managers and auditors: (1) create a control environment that addresses the overall culture of the company; (2) assess the most critical risks to internal controls; (3) create control structures that outline important processes and guidelines; (4) provide clear information about employees' responsibilities and procedures to be followed; and (5) monitor internal controls. The Sarbanes–Oxley Act requires public companies to define their control framework and specifically recommends COSO as that business framework for general accounting controls. It is not IT specific.

[25] Ben Worthen, "The Top Five IT Control Weaknesses" (July 1, 2005), http://www.cio.com/article/2448687/project-management/the-top-five-it-control-weaknesses.html (accessed September 4, 2015).

COBIT

Control Objectives for Information and Related Technology (COBIT) COBIT (Control Objectives for Information and Related Technology) is an IT governance framework that is consistent with COSO controls, and also a governance tool to ensure that IT provides the systematic rigor needed for the strong internal controls and Sarbanes–Oxley compliance. It provides a framework for linking IT processes, IT resources, and IT information to a company's strategies and objectives. As a governance framework, it provides guidelines about who in the organization should make decisions about IT processes, resources, and information.

Information Systems Audit & Control Association (ISACA) issued COBIT in 1996. COBIT consists of several overlapping sets of guidance with multiple components, which almost form a cascade of process goals, metrics, and practices. At the highest level, key areas of risks are defined in four major domains: planning and organization, acquisition and implementation, delivery and support, and monitoring and evaluating. When implementing a COBIT framework, a company determines the processes that are the most susceptible to the risks that it judiciously chooses to manage. There are far too many risks for a company to try to manage all of them.

Once the company identifies processes that it is going to manage, it sets up a control objective and then more specific key goal indicators. As with any control system, metrics called *key performance indicators (KPIs)* need to be established to enable measurement of progress in meeting the goals. Then activities to achieve the KPIs are selected. These activities, or *critical success factors*, are the steps that need to be followed to successfully provide controls for a selected process. When a company wants to compare itself with other organizations, it uses a well-defined maturity model. The components of COBIT and examples of each component are provided in Figure 9.8.

One advantage of COBIT is that it is well suited to organizations focused on risk management and mitigation. Another advantage is that it is very detailed. However, this high level of detail unfortunately can serve as a disadvantage in the sense that it makes COBIT very costly and time consuming to implement. Yet, despite the costs, companies are starting to realize benefits from its implementation. As a governance framework, it designates clear ownership and responsibility for key organizational processes in such a way that is understood by all organizational

Component	Description	Example
Domain	One of four major areas of risk: plan and organize (PO), acquire and implement (AI), deliver and support (DS), and monitor and evaluate (ME); each domain consists of multiple processes	Deliver and support (or DS)
Control objective	Focus on control of a process associated with risk; can be 34 processes	DS (deliver and support) objective #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 have been met in regard to a control objective	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: percentage should decrease over specified periods of time)
Critical success factor	Description of the steps that a company must take to accomplish a control objective; can be 318 critical success factors	Data entry requirements 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	Level 0: Data not recognized as corporate resources and assets; no assigned data ownership or individual accountability for data integrity and reliability; data quality and security poor or nonexistent

FIGURE 9.8 Components of COBIT and their examples.
Source: Adapted from Hugh Taylor, *The Joy of SoX* (Indianapolis, IN: Wiley, 2006).

stakeholders. Consistent with the Information Systems Strategy Triangle discussed in Chapter 1, COBIT provides a formal framework for aligning IS strategy with the business strategy. It does so by using a governance framework and focusing on risks of internal control and associated processes to recognize who is responsible for important control decisions. Finally, COBIT makes possible the fulfillment of the COSO requirements for the IT control environment that is encouraged by the Sarbanes–Oxley Act.

Other Control Frameworks

Although COBIT is the most common set of IT control guidelines for SoX, it is by no means the only control framework. Others include those provided by the International Standards Organization (ISO), as well as the **Information Technology Infrastructure Library (ITIL)**. A set of concepts and techniques for managing information technology infrastructure, development, and operations, ITIL was developed in the United Kingdom. It is a widely recognized framework for IT service management and operations management that has been adopted around the globe. ITIL 2011 has five distinct volumes: service strategy; service design; service transition; service operation; and continual service improvement.

IS and the Implementation of Sarbanes–Oxley Act Compliance

Because of the level of detail, the involvement of the IS department and the CIO in implementing SoX—most notably Section 404, which deals with management's assessment of internal controls—is considerable. Although the IS department typically plays a major role in SoX compliance, it often lacks formal authority. Thus, the CIO needs to tread carefully when working with auditors, the CFO, the CEO, and business leaders. Braganza and Franken provide six tactics that CIOs can use in working effectively in these relationships. These strategies include knowledge building, knowledge deployment, innovation directive, mobilization, standardization, and subsidy. Figure 9.9 provides a definition for each of these tactics, along with examples of activities to enact them.

Tactic	Definition	Examples of Activities
Knowledge building	Establish a knowledge base to implement SoX	Acquire technical knowledge about SoX and Section 404
Knowledge deployment	Disseminate knowledge about SoX and develop an understanding of this knowledge by management and other organizational members	Move IT staff with knowledge of 404 to parts of the organization that are less knowledgeable; create a central repository of 404 knowledge; absorb 404 requirements from external bodies; conduct training programs to spread an understanding of SoX
Innovation directive	Organize for implementing SoX and announce the approach	Issue instructions that encourage the adoption of 404 compliance practices; publish reports of each unit's progress toward implementation; deploy drivers for implementation; direct implementation from top down and/or bottom up
Mobilization	Persuade decentralized players and subsidiaries to participate in SoX implementation	Create a positive impression of SoX (and 404) implementation; conduct promotional and awareness campaigns
Standardization	Negotiate agreements between organizational members to facilitate the SoX implementation	Use mandatory controls, often embedded within the technology; indicate formal levels of compliance required; establish *firmwide* standards of control; create an overarching corporate compliance architecture
Subsidy	Fund the implementers' costs during the SoX implementation and the users' costs during its deployment and use	Centralize template development; develop Web-based resources; train IT staff for implementing 404; fund short-term skill gaps; track implementation; target funds during implementation for specific IT-related 404 goals

FIGURE 9.9 CIO tactics for implementing SoX compliance.
Source: Adapted from Ashley Braganza and Arnoud Franken, "SoX, Compliance, and Power Relationships," *Communications of the ACM* 50, no. 9 (September 2007), 97–102.

Social Business Lens: Governing the Content

Since the beginning of social applications like Facebook, Twitter, and Instagram, there has been a debate about who gets to decide on what's allowed to be posted. Should the users decide? Should the application company decide? This debate still rages today.

One perspective is that the users own and manage their content. Aside from the legal issues, which are discussed in Chapter 13 of this text, users have control over what they post and what they block from their pages on most social media. Most social networks have controls that allow users to block others from posting on their page, but it's not the default in most cases. For example, when a user tags another Facebook user in a post or photo, the content then also shows up on the tagged person's timeline. Even though a control can be set to minimize this, some have found it troublesome that items can be placed in their timeline in this manner. Most users feel that they should have control of their content on their social media page.

Now ratchet this up to the group level. Should the "crowd" decide what is appropriate to put on a social media site or should the company decide? The crowd has a say in some manner; members of the community can vote or "like" a post and in some cases, content with the most votes rises to the top for others to see.

But the social media company also has a say in what content is appropriate. Again, aside from content that crosses legal boundaries, which of course vary country by country, some companies have taken a stronger stance. For example, Instagram removed a number of users from its Web site for not following instructions. Its Web site plainly stated two new policies:

We want Instagram to continue to be an authentic and safe place for inspiration and expression. Help us foster this community. Post only your own photos and videos and always follow the law. Respect everyone on Instagram, don't spam people or post nudity.*

We want . . . to maintain the best possible experience on Instagram, so spam, fake accounts and other people and posts that don't follow our Community Guidelines may be removed from Instagram.†

*From Instagram's Community Guidelines, https://help.instagram.com/477434105621119/ (accessed May 22, 2015).
†From Instagram's Help Center, https://help.instagram.com/309501049246773 (accessed May 22, 2015).

Sources: "Chaos Ensues As Instagram Deletes Millions of Accounts," http://www.businessinsider.com/chaos-ensues-as-instagram-deletes-millions-of-accounts-2014-12#ixzz3MIXUmldn (accessed September 4, 2015); and Instagram company website, www.instagram.com; "Instagram Users Report Mass Deletion of Profiles for 'violating' Terms of Service," http://tech.firstpost.com/news-analysis/instagram-users-report-mass-deletion-of-profiles-for-violating-terms-of-service-86660.html (accessed September 4, 2015); "Instagram Deletes Millions of Accounts in Spam Purge," http://www.bbc.com/news/technology-30548463 (accessed September 4, 2015).

The extent to which a CIO could use these various tactics depends on the power that he or she holds relating to the SoX implementation. Those few CIOs who are given carte blanche by their CEOs to implement SoX compliance can employ compelling activities, such as subsidy, standardization, and innovation directives. Those CIOs can establish standards and enforce their compliance, creating an overarching corporate compliance architecture. They can direct the SoX implementation from top down and put Section 404 implementation drivers in place. If, on the other hand, the CEO does not vest the CIO with the considerable power to employ such tactics, the CIO may need to take more of a persuasive stance and focus on training programs and building an electronic knowledge database of SoX documents. In this case, it is especially important to sell the CIO and CFO on the importance of complying with prescribed procedures and methods. In either situation, the CIO needs to acquire and manage the considerable IT resources to make SoX compliance a reality.

These new guidelines sound reasonable enough, but they are much more stringent than the previous set of guidelines they replaced. Instagram deleted not only thousands of accounts, which mostly involved spam and fake identities, but also others that the company deemed inappropriate. According to some sources, the crowd was not happy. A mass campaign to stop following Instagram's own official Instagram account followed, and that account lost 30% of its followers. Does the crowd govern the content or the company?

SUMMARY

- Alternative approaches to governance of information systems organization are possible. One approach is based on where IS decisions are made in the organization's structure. Centralized IS organizations place IT staff, hardware, software, and data in one location to promote control and efficiency. At the other end of the continuum, decentralized IS organizations with distributed resources can best meet the needs of local users. Federalism in IS organizations is in the middle of the centralization/decentralization continuum.
- A second governance approach involves decision rights. In this approach, IT governance specifies how to allocate decision rights in such a way as to encourage desirable behavior in the use of IT. The allocation of decision rights can be broken down into six archetypes (business monarchy, IT monarchy, feudal, federal, IT duopoly, and anarchy). High-performing companies use the proper decision rights allocation patterns for each of the five major categories of IT decisions.
- A third governance approach recognizes the power of combining complementary technologies in ways that were not predicted or controlled by an organization. This so-called digital ecosystem represents formal recognition of a firm's healthy adaptation and synergistic adoption to new hardware, applications, and connections with customers, employees, and other firms. Much of this has been driven by consumerization of technology.
- A fourth governance approach is based on controls. The Sarbanes–Oxley Act (2002) was enacted to improve organizations' internal controls. COBIT is an IT governance framework based on control that can be used to promote IT-related internal controls and Sarbanes–Oxley compliance.

KEY TERMS

archetype (p. 196)
centralized IS organizations (p. 193)
COBIT (Control Objectives for Information and Related Technology) (p. 202)
Consumerization (p. 191)
decentralized IS organizations (p. 193)
digital ecosystem (p. 197)
federalism (p. 194)
governance (p. 192)
Information Technology Infrastructure Library (ITIL) (p. 203)
IT governance (p. 195)
review board (p. 199)
Sarbanes–Oxley Act (SoX) (p. 200)
steering committee (p. 199)

DISCUSSION QUESTIONS

1. The debate about centralization and decentralization is heating up again with the advent of BYOD and the increasing use of the Web. Why does the Internet make this debate topical?
2. Why is the discussion of decision rights among managers in a firm important?
3. Why can an IT governance archetype be good for one type of IS decision but not for another?

■ CASE STUDY 9-1 IT Governance at University of the Southeast

University of the Southeast[25] was (and still is) one of the largest universities in the United States. It had been growing rapidly; that growth was spurred, in part, by information technology. The university embraced lecture capture technologies that allowed lectures to be streamed to students in a classroom, in dorm rooms, on the grass near the main campus central fountain, and at a variety of other places of the students' choosing whenever they chose to watch. This made it possible to have sections of classes with over 1,000 students without having to build physical classrooms with enough seats to accommodate each person enrolled. It also made it possible to offer classes that were streamed to students at remote campuses. Each student was charged a technology fee (i.e., $5.16 for undergraduates and $13.85 for graduates per credit hour each semester), which was administered by the Information Technologies and Resources (IT&R) Office to help fund the costs of providing IT to students and faculty.

[25] The name University of the Southeast is made up but the school and situation were real.

IT&R was responsible for providing computer services, technologies, and telecommunications across the campus (Computer Services and Technology), helping faculty with their instructional delivery and multimedia support (Office of Instructional Resources), helping faculty develop and deliver Web-based and lecture capture courses (Center for Distributed Learning), and the library. The IT&R Office developed IT-related policies with very little input from the faculty and was responsible for deciding and implementing decisions concerning IT architecture and infrastructure. IT&R worked with the university president and other top administrators in making IT investment decisions. IT&R staff also worked with the various colleges, administrative offices, and an advisory board in making decisions about applications that needed to be developed. However, faculty were not consulted at all when the lecture capture system was selected.

As was often the case at large universities, many decision rights on a wide range of issues had been allocated to the colleges. The College of Business Administration had its own server and Technology Support Department (TSD). A recent survey of faculty and staff in the college indicated a high level of satisfaction with the TSD but far less satisfaction with the services provided by the university-level IT&R. Some college respondents indicated their displeasure about IT&R's support of the technology for the lecture capture courses, help desk, and classroom technologies.

The problems with the technology support for lecture capture software were particularly troublesome. The software would not authenticate students who had paid to enroll in some lecture capture courses, making it impossible for them to download the lectures even though they were registered in the course. Further, some university-affiliated housing did not have adequate network bandwidth to allow students to download the lectures. When problems occurred—which they did on a daily basis—the IT&R help desk often referred the students to instructors who could not resolve their problems. One faculty member who was teaching a lecture class with 1,400 students exclaimed, "It is utter chaos for me when something goes wrong with the system and hundreds of my students are trying to call, see or email me in panic to get me to fix something that I can't fix."

To fix some of these issues, the CIO argued that all e-mail accounts should be placed on one central server. This would allow the IT&R greater control and make maintenance easier and more efficient. It also would considerably improve security. But it was not ideal for the faculty. A faculty meeting about e-mail revealed some concerns with this move. First, faculty wanted e-mails sent to the central university server to be forwarded to their accounts on their other university-based servers (i.e., the college, department, or institute servers) but found that this was impossible to do so. Second, faculty wanted to retain their control over archiving e-mails. Third, faculty wanted to have control over their preferred e-mail address. In some cases, the faculty e-mail addresses that they had used for a decade had been changed in the printed university directory to the e-mail address on the central university server without their knowledge. This meant that faculty did not receive (or even know about) messages sent to them via the address on the university server. They could not change the printed e-mail address in the university directory to the address on the college server that they had been using or forward the mail sent to the central server to a different account.

The IT&R spokesman said that having a centralized server for e-mail accounts was more secure, reliable and efficient. He said that faculty shouldn't have control over their preferred e-mail address, even if it were on a campus server, because of the identity management problems that it would create. A frustrated faculty member at the meeting asked the IT&R spokesman to describe one time when issues about ease of use and functionality of the system by the user were weighted more than security in decisions about e-mail. The IT&R spokesman could not think of an example.

Discussion Questions

1. Describe the IT governance system that was in place at the University of the Southeast using both decision rights and structure as the bases of governance.
2. The CIO wanted to implement a centralized IT governance system. As demonstrated in this case, what are the advantages of a centralized IT governance system? What are the disadvantages?
3. In your opinion, what assignment of decision rights would be best for University of the Southeast? Please explain.