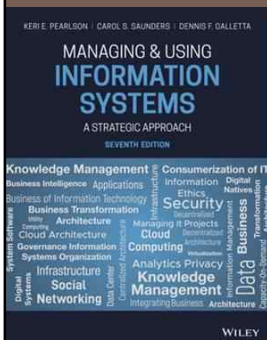


CHAPTER 9

GOVERNANCE OF THE INFORMATION SYSTEMS ORGANIZATION



Managing & Using Information Systems: A Strategic Approach (7th Edition),
 Pearlson, Saunders, & Galletta

Chapter Introduction

2

- **Governance structures** define the way decisions are made in an organization.
- This chapter explores **four models of governance** based on:
 1. The location of decision making in organization structure (centralized, decentralized, and federal)
 2. Decision rights
 3. Digital ecosystems
 4. Control



Chapter Introduction

3

- Considering frameworks from:
 - The Committee of Sponsoring Organizations of the Treadway Commission (COSO)
 - Control Objectives for Information and Related Technology (COBIT)
 - Information Technology Infrastructure Library (ITIL)
- Examples and strategies for implementation are discussed.

COSO ERM Framework

COBIT
An ISACA® Framework

ITIL FRAMEWORK

CASE: Intel's Transformation

4

- Intel's information technology (IT) performance reports for 2013 and 2019 boast about how the company **increased** its storage capacity **from** 25 petabytes in 2010 **to** 315 petabytes in 2018, and over the same interval **raised** the number of handheld devices **from** 19,400 **to** over 210,000.
- Intel also exploited other highly visible opportunities of using predictive data analytics, Internet of Things (IoT) technology and smart factories.



NAME	FACTOR	VALUE IN BYTES
kilobyte	10 ³	1,000
megabyte	10 ⁶	1,000,000
gigabyte	10 ⁹	1,000,000,000
terabyte	10 ¹²	1,000,000,000,000
petabyte	10 ¹⁵	1,000,000,000,000,000
exabyte	10 ¹⁸	1,000,000,000,000,000,000
zettabyte	10 ²¹	1,000,000,000,000,000,000,000
yottabyte	10 ²⁴	1,000,000,000,000,000,000,000,000

CASE: Intel's Transformation

5

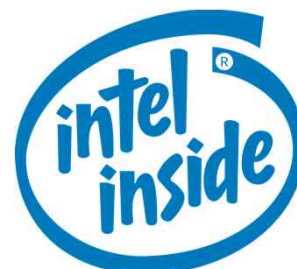
- Consequently, Intel was able to develop such **far-ranging** (광범위한) applications as digital supply chains, smart buildings, and wearable analytics platforms.
- An outsider might assume that Intel stepped up spending and IT investments to accomplish these goals.
- However, it actually **reduced** the number of data centers **from** 91 in 2010 **to** 55 in 2018 (even while adding two ultra-high efficiency data centers) and **reduced** IT spending **from** 2.64% **to** 2.30% of revenue during that same eight-year interval.



CASE: Intel's Transformation

6

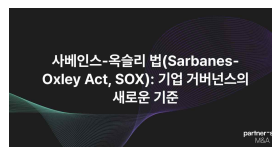
- How did Intel accomplish these and other **laudable** (praiseworthy) goals?
- Its approach was the result of 25 years of evolution of its strategy that began by creating a centralized IT organization in 1992 with control **resting in** (...에 원인이 있다) IT.
- Intel has come a long way from its original governance structure, which was centered on mainframes and wide-area networks.



CASE: Intel's Transformation

7

- 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** (**해결책**) to be able to complete some of their tasks.
- Data could be used only within a particular functional area, not shared among areas.



CASE: Intel's Transformation

8

- 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 (**damaging**) to innovation over the long run.
- This led Intel to discover that **consumerization** is a powerful force.
- That six-syllable mouthful (**consumerization**) describes the increasingly powerful tools available in the consumer space that can impact the corporate space.

CASE: Intel's Transformation

9

- **IT consumerization** is "the process whereby the changing practices and expectation of consumers, shaped by the wide adoption of digital technologies in everyday life, will influence the IT-related activities of workers and managers in organizations."
- The consumers in this case are **not only** customers (consumer-customers) **but also** workers in organizations (consumer-workers) whose work practices are shaped by their experiences with the digital technologies that they use in their daily lives.



CASE: Intel's Transformation

10

- Mobility has been the major breakthrough in consumerization, and **the increasing use** of smartphones, tablets, and smaller/more powerful laptops coupled with web-based applications that offer everything **from** free business productivity tools (e.g. Google Docs), **to** sharing applications (e.g. YouTube, SlideShare) and **to** social tools (e.g. Twitter, 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.

CASE: Intel's Transformation

11

- 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 **from** "How do we stop it' **to** "How do we work with this?"

CASE: Intel's Transformation

12

- Intel's governance structure also resulted in a lost opportunity to exploit data and analytics.
- 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 Era" has addressed **(deal with)** those needs.

CASE: Intel's Transformation

13

- More recently, Intel has extended the governance framework's reach (scope) by focusing on IT innovation to transform business value.
- Intel boasts of saving 933,000 hours per quarter in improved productivity, improved time to market for platforms, and adding \$2.85 billion in top-line revenue.
- Productivity was improved by **using** a new Intel "Unite" solution, **instituting** one-click video meetings, **installing** "Grab N Go" PC lockers, **creating** self-healing virtual private networks, and **adding** new mobile capabilities.

CASE: Intel's Transformation

14

- Intel also improved **time to market** new platforms and designs by adopting machine learning and smart analytics.
- The "Unite" initiative allows **wireless connections** of "all major devices, operating systems, and displays" **with** its open platform.
- That move led Intel to **move from** 2,700 collaboration rooms in 2016 **to** 5,300 in 2018 and helps keep employees communicating with ease.

CASE: Intel's Transformation

15

- 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.



CASE: Intel's Transformation

16

- **Sharing** the governance **with** business units is one of five "key success factors," according to an analysis of the Intel case.
- 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."

- **Disrupt:** (of a company or form of technology) cause radical change in (an industry or market) by means of innovation



IT Governance

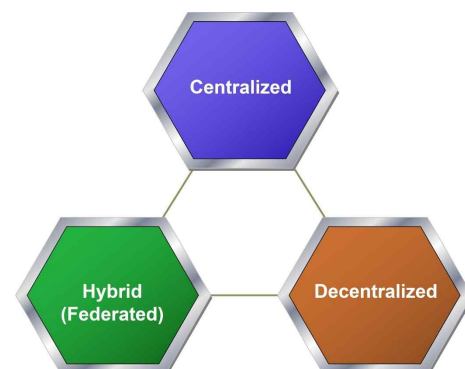
17

- Governance (in business) is all about making decisions that
 - Define expectations
 - Grant authority
 - Ensure performance
- Empowerment and monitoring will help align behavior with business goals.
 - **Empowerment:** Granting the right to make decisions.
 - **Monitoring:** Evaluating performance.

IT Governance

18

- IT governance focuses on how decision rights can be distributed differently to facilitate three possible modes of decision making:
 - Centralized
 - Decentralized
 - Hybrid (Federated)
- Organizational structure plays a major role.



Four Perspectives

19

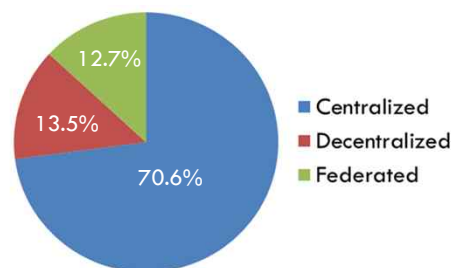
1. Traditional – Centralized vs Decentralized.
2. Accountability and allocation of decision rights.
3. **Ecosystem** reflecting the significant impacts of the large variety of resources.
4. Control structures from legislation.



Organizational Structural Approaches

20

- **Centralized:** Bring together all staff, hardware, software, data, and processing into a single location.
- **Decentralized:** The components in the centralized structure are scattered in different locations to address local business needs.
- **Federalism:** A hybrid of centralized and decentralized structures.
- Recent global survey:
 - Centralized: 70.6%
 - Decentralized: 13.5%
 - Federated: 12.7%



Organizational Structural Approaches

21

- Figure 9.1 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.

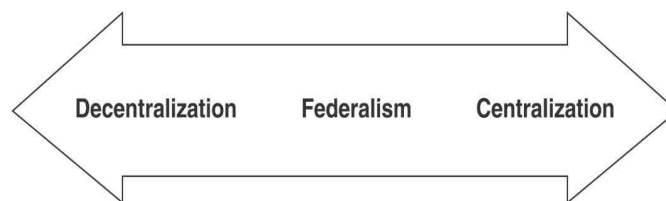


Figure 9.1 Organizational Continuum

Organizational Structural Approaches

22

- Figure 9.2 shows advantages and disadvantages of each organizational approach.
- Most companies want to achieve the advantages derived from both organizational paradigms.

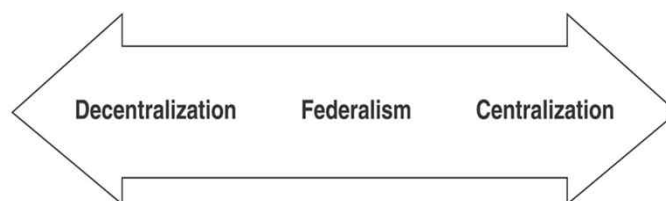


Figure 9.1 Organizational Continuum

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 (분립) between business and IT organization "Us versus them" mentality (사고방식) when technology problems occur - Lack of business unit control over overhead costs	UPS

Figure 9.2.1 Advantages and Disadvantages of Organizational Approaches

23

Approach	Advantages	Disadvantages	Companies Adopting
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 (우선권[특혜]을 주는) supplier agreements - Loss of control - Duplication of staff and data	Fedex

Figure 9.2.2 Advantages and Disadvantages of Organizational Approaches

24

Organizational Structural Approaches

25

- **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 9.3 shows how these approaches interrelate.

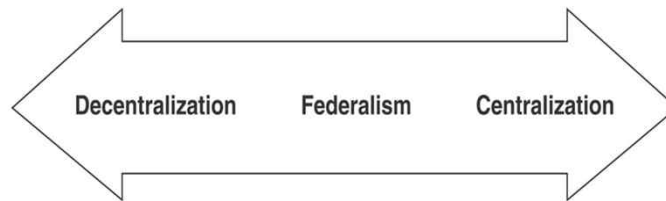


Figure 9.1 Organizational Continuum

Organizational Structural Approaches

26

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

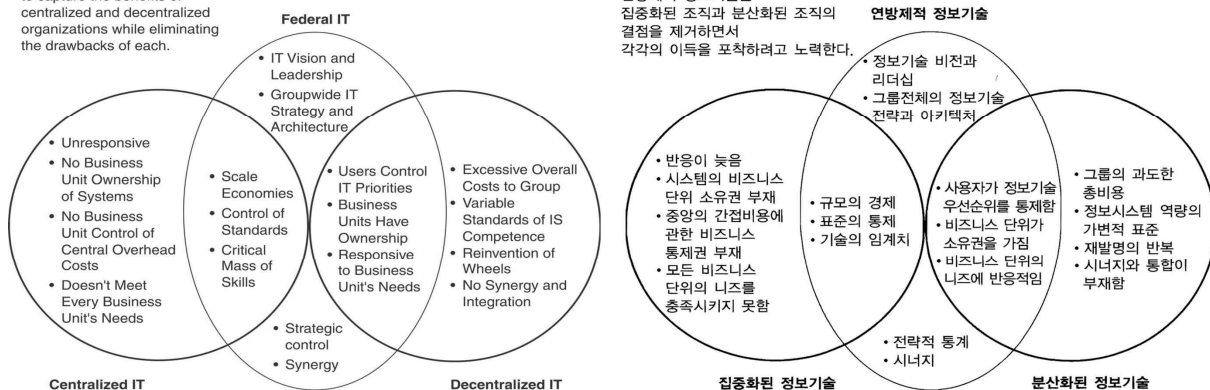


Figure 9.3 Federal IT

Decision Rights and Governance

27

- 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.



Decision Rights and Governance

28

- **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.
- **Mismatches** result in **either** an oversupply of IT resources **or** the inability of IT to meet business demand.



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 • Figure 8.1.1 & 8.1.2
	Low	Support Norm (Level 1 balance) • It works for organizations where IT is viewed as a support function • Its focus is on business efficiency • Figure 8.1.1 & 8.1.2	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.

29

Maturity Level	Nature of the Level	Engagement Characteristics
Level 3	• IT as business partner	• Proactive • Outside-in • Relationship centric • Focused on business growth • Framed in a context of business value
Level 2	• IT as solutions provider	• Active • Process centric • Focused on solutions • Framed in a context of projects
Level 1	• IT as order taker	• Reactive • Inside-out • Technology centric • Framed in a context of cost

Figure 8.1.1 Business-IT Maturity Model

30

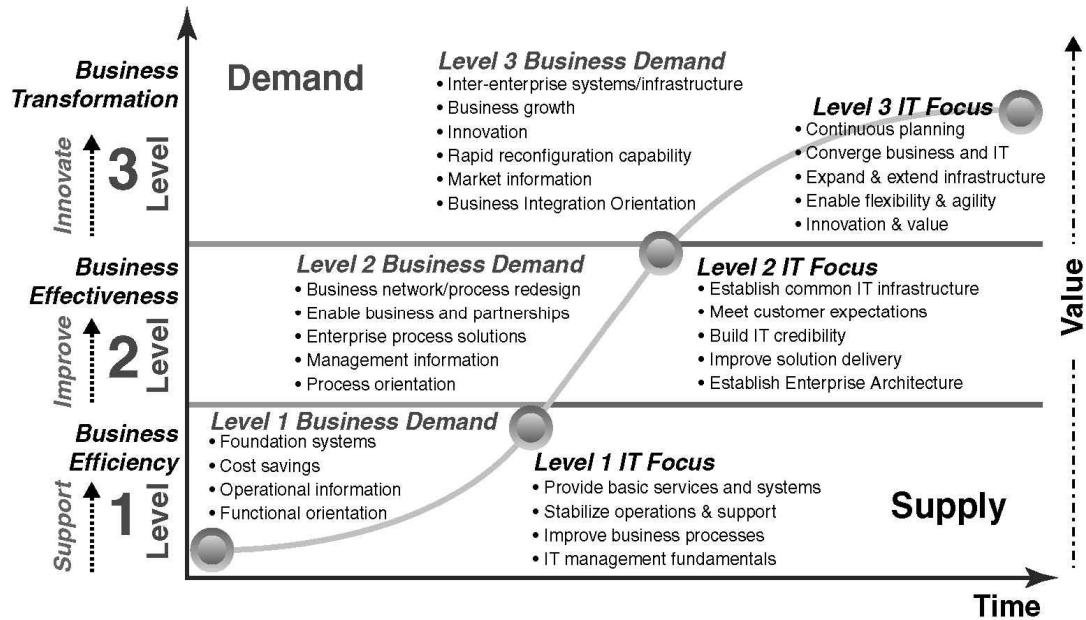
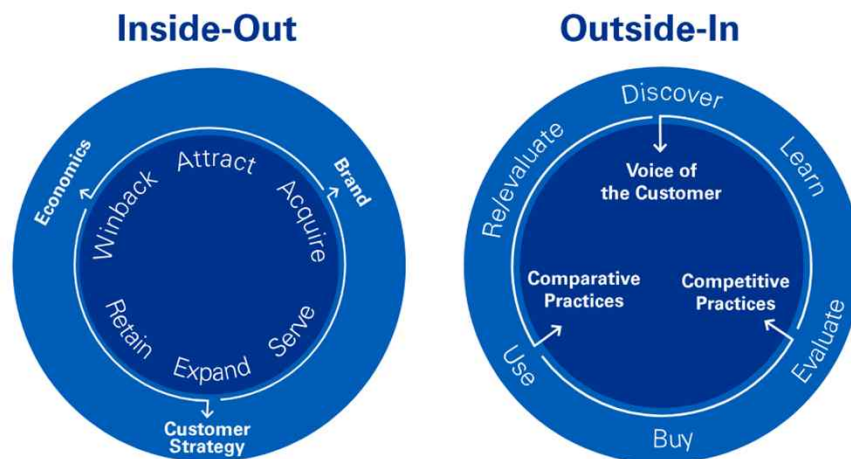


Figure 8.1.2 Business-IT Maturity Model

31

“Inside-Out” and “Outside-In” Approach to Doing Business

32



“Inside-Out” and “Outside-In” Approach to Doing Business

33

Inside-Out

- What's the product we are offering?
- What business processes will we implement that customers will use to complete this transaction?
- What other information do we need from the customer so we can complete this transaction?
- What can we do to get similar customers?

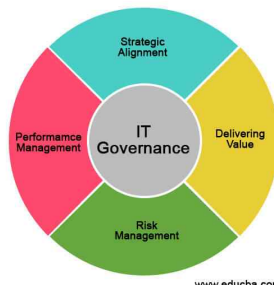
Outside-In

- What's my customer's true need and what interactions can I create to make it easier?
- What does our customer actually need right now?
- Can the customer accomplish what they need across multiple channels easily?
- What other products, information or suggestions can we provide that offer real value now and in the future?

Decision Rights and Governance

34

- Good IT governance provides a structure to make good decisions.
- IT governance has two major components:
 - The assignment of **decision-making authority** and **responsibility**.
 - The decision-making mechanisms (e.g., steering committees, review boards, policies).



Decision Rights and Governance

35

- Weill and his colleagues proposed five generally applicable categories of IT decisions:
 - IT principles
 - IT architecture
 - IT infrastructure strategies
 - Business application needs
 - Investment and prioritization.
- Figure 9.5 **provides** a description of these decision categories **with** an example of major IS activities affected by them.

Decision Rights and Governance

36

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

Archetypes of Accountability and Decision Rights

37

- Weill and Ross propose **archetypes** labeling the combinations of people who either input information or have decision rights for key IT decisions.
 - Business monarchy: 비즈니스 군주형/비즈니스 주도형
 - IT monarchy: IT 군주형/IT 주도형
 - Feudal: 봉건형/현업 주도형
 - Federal: 연방형/관리부서-현업 연방형
 - IT duopoly: 독점형/IT-비즈니스 조합형
 - Anarchy: 무정부형/개별 사용자 주도형
- Archetype(전형): a perfect example of something

Archetypes of Accountability and Decision Rights

38

- An **archetype** is a pattern for decision rights allocation.
- Decisions can be made at several levels in the organization (Figure 9.6).
 - Enterprise-wide,
 - Business unit, and
 - Region/Group within a business unit.

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 비즈니스 군주형 / 비즈니스 주도형	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 IT 군주형/IT 주도형	Individuals or groups of IT executives.		✓	
Feudal 봉건형/역역 주도형 / 군림	Business unit leaders, key process owners or their delegates.			✓
Federal 연방형 / 관리형, 역역 연합형	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 독점형 / IT-비즈니스 조함형	IT executives and one other group (e.g., CxO or BU leaders).	✓	✓	
			✓	✓
Anarchy 무정부형 / 개별 사용자 주도형	Each individual user.			

© MIT Sloan Center for Information Systems Research 2003 - Weill

Figure 9.6.1 IT Governance Archetypes

39

대상 주체	IT 원칙	IT 아키텍처	IT 인프라 전략	비즈니스 애플리케이션 요구	IT 투자와 우선 순위
비즈니스 군주형					
IT 군주형					
봉건형					
연방형					
복점형					
무정부형					

Figure 9.6.2 IT Governance Archetypes

40

Archetypes of Accountability and Decision Rights

41

- There is significant variation across organizations in terms of archetypes selected for decision right allocation.
 - The IT duopoly (복점형/IT-비즈니스 조합형) is used by the largest portion (36%) of organizations for IT principles decisions.
 - IT monarchy (IT 군주형/IT 주도형) is the most popular for IT architecture (73%) and infrastructure decisions (59%).

대상 주체	IT 원칙	IT 아키텍처	IT 인프라 전략	비즈니스 애플리케이션 요구	IT 투자와 우선 순위
비즈니스 군주형					
IT 군주형		73%	59%		
봉건형					
연방형					
복점형	36%				
무정부형					

Figure 9.6.3 IT Governance Archetypes

42

Decision-Making Mechanisms

43

- In one worldwide study of IT governance, almost 60% of the respondents relied on **policies and standards**, making it the most popular mechanism for governance.
- 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.
- A third mechanism that is used very frequently for IT decisions is the **IT steering committee**, also called an **IT governance council**.

Platform-Based Governance

44

- The technology at the heart of digital ecosystems and, to a great extent, **IT consumerization**, is the digital platform.
- A **digital platform** is “a layered architecture of digital technology combined with a governance model.”
- The governance model affects the growth of the ecosystem and the success of the platform.
- A fancy term, often used to describe digital platforms, is **generativity** (생식성), or “the ability of any self-contained system to create, generate, or produce a new output, structure, or behavior without any input from the originator of the system.”
- **Generativity** (the ability to create or reproduce) is very important for digital ecosystems.



Digital Ecosystems

45

- Digital ecosystems **regard** those systems **as** self-interested, self-organizing, and autonomous digital entities.
- In essence, this means that a digital ecosystem is nourished by the significant impacts of **the large variety of resources** available from individuals, organizational units, and outside services.
- In recent years, mobile computing, GPS, and social media have indeed presented new, unexpected challenges and opportunities.

Digital Ecosystems

46

- However, other technological developments have also provided digital ecosystem opportunities, such as cloud computing, the IoT, **edge computing**, radio frequency ID (RFID), and smart cards.
- A smartphone provides another example of how a digital ecosystem can form between applications, firms, and digital entities.



Digital Ecosystems

47

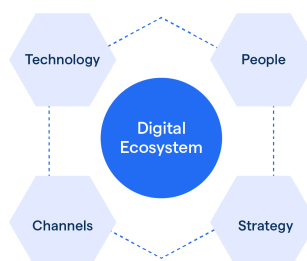
- Strong governance implications emerge from digital ecosystems.
- The symbiotic (공생의) multi-firm and adaptive situations cannot be completely planned or orchestrated by a single entity.
- Much of the decision making exists outside the firm, and, therefore, complete plans no longer can be made in a single boardroom.
- Platform participants often find themselves moving in directions that could not be predicted.



Digital Ecosystems

48

- **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 would need to be changed in mid-year to **take advantage of** sudden new technological opportunities or challenges.
- Competitors could suddenly become allies, or vice-versa.



Digital Ecosystems

49

- Business processes would need to change quickly.
- New capabilities that might be contrary to previous activities or directions might need to be enabled quickly.
- Firms in the future will probably need to address all these situations for their ultimate survival.



IT Consumerization

50

- In addition to digital ecosystems, **platform-based governance** plays an important role in IT consumerization.
- **IT consumerization** is based on the concept of “everyone's IT” and characterized by the individualization of IT and the democratization of IT access.



IT Consumerization

51

- IT consumerization is such a powerful force that it is **transforming** traditional IT governance that focuses on an organization's assets **into** a platform-based governance that capitalizes on resources from the external environment.
- **The scope of platform-based governance** is on autonomous cross-functional teams that can develop applications without the aid of IT professionals.

[Service Management Blog](#)

What Is Consumerization of IT?
 The State of Consumerization of
 IT

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.
Platform-based	- Members of the ecosystem contribute their strengths, giving the whole ecosystem a complete set of capabilities that can impact decision making and operations. - IT consumerization results in cross-functional teams that have direct, unmediated access to IT using platforms that promote combinations of assorted digital technologies and resources.	Build generativity, flexibility and adaptability into governance.

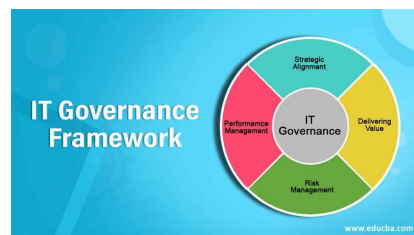
Figure 9.7 Three Governance Frameworks

52

Governance Frameworks for Control Decisions

53

- Recently, governance frameworks have been employed specifically to define **responsibility for control decisions** and help ward off (**prevent**) future accounting fiascos (**a complete failure or disaster**).
- These frameworks focus on **processes** defined by legislation and describe **risks** associated with them.



Sarbanes–Oxley Act of 2002

54

- 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 (Securities & Exchange Commission: 증권거래위원회) are subject to SoX requirements.
- CEOs** and **CFOs** must personally certify and be accountable for their firm's financial records and accounting.

사베인스 옥슬리법

문서 토론

위키백과, 우리 모두의 백과사전.

사베인스-옥슬리 법(Sarbanes-Oxley Act, SOx, Pub.L. 107-204 4, 116 Stat. 745, 2002년 7월 30일 발효)은 "상장회사 회계 개선과 투자자 보호법"(상원) 또는 "법인과 회계 감사 책임 법"(하원) 또는 Sarbox or SOX로도 불리는 미국의 회계 개혁에 관한 연방법률로서, 월드콧과 앤슨같은 거대 기업들의 잇달은 회계 부정으로 인해 막대한 피해가 발생하자 회계제도 개혁의 필요성이 제기되었고, 2002년 7월 30일 법안의 발의자인 상원의원 톰 사베인스(민주당, 매릴랜드)와 하원의원 마이클 옥슬리(공화당, 오하이오)의 이름을 따서 제정되었다.

SoX - Financial Controls

55

- **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

56

- Five IT control weaknesses are repeatedly uncovered by auditors:
 1. **Failure to segregate** (separate) 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.

Frameworks for Implementing SoX

57

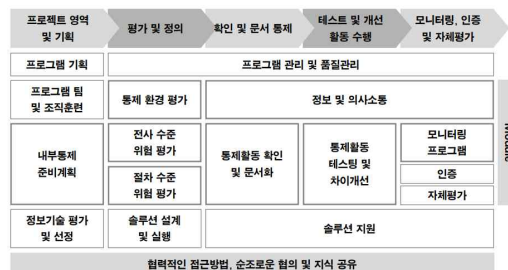
- Several different commissions, committees, and frameworks are important for understanding SoX.
- Below we describe the committee that
 - Created relevant control objectives and components (COSO), as well as
 - Introduce COBIT and other control frameworks.

COSO

58

- 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)*.

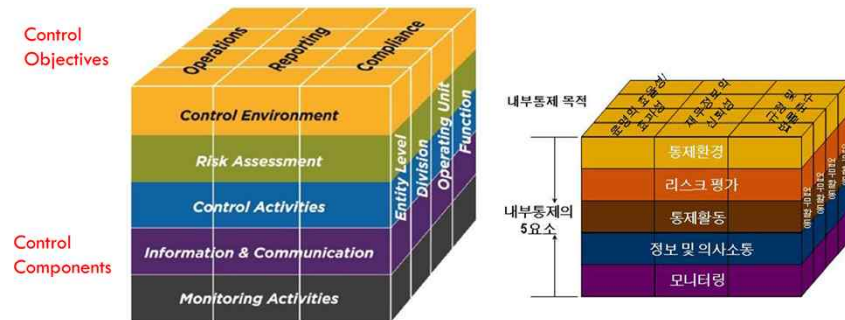
미국 테네시(Tennessee)주 헨콕 카운티(Hancock County)에 있는 자치구



COSO

59

- They created three **control objectives** for management and auditors that focused on dealing with **risks to internal control**.
- These control objectives cover operations, compliance, and financial reporting.



COSO

60

Control Objectives

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, 일반회계원칙). • SoX is focused on this control objective.

**회계원칙
(GAAP)**

COSO

61

Control Components

Control Environment	• Create a control environment that addresses the overall culture of the company.
Risk Assessment	• Assess the most critical risks to internal controls.
Control Activities	• Create control structures that outline important processes and guidelines.
Information & Communication	• Provide clear information about employees' responsibilities and procedures to be followed.
Monitoring Activities	• Monitor internal controls.

COSO

62

- SoX:
 - Requires public companies to define their **control framework**.
 - Recommends COSO as the business framework for general accounting controls.
 - Is not IT-specific.



COBIT

63

- COBIT (Control Objectives for Information and Related Technology) 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.



COBIT

64

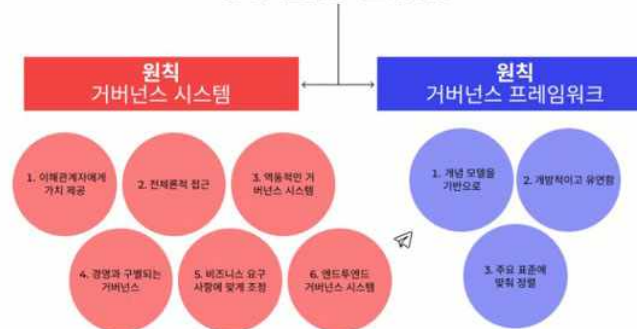
- COBIT provides a set of process goals, metrics, and practices.
 - Risk categorized into four major domains:
 - ✓ Planning and organization
 - ✓ Acquisition and implementation
 - ✓ Delivery and support
 - ✓ Monitoring
 - The company determines the processes that are the most susceptible to the **risks** that it chooses to manage.

COBIT

65

- The company identifies **processes** that it is going to manage.
- Sets up a **control objective** and more specific key goal indicators.

COBIT 2019



COBIT

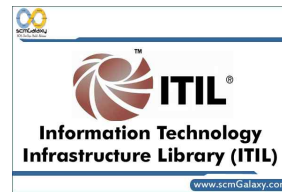
66

- 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

67

- 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.
 - A widely recognized framework for IT service management and operations management that has been adopted around the globe.



Five Phases of ITIL Process Life Cycle

68



IS and the Implementation of SoX Act Compliance

69

- 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 9.8):

1. Knowledge Building
2. Knowledge Deployment
3. Innovation Directive
4. Mobilization
5. Standardization
6. Subsidy



IS and the Implementation of SoX Act Compliance

70

Tactic	Definition	Examples of Activities
Knowledge Building	• Establish a knowledge base to implement SoX.	• Acquire technical knowledge about SoX and 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.

Figure 9.8.1 CIO Tactics for Implementing SoX Compliance

Tactic	Definition	Examples of Activities
Innovation Directive	Organize for implementing SoX and announce the approach.	- Issue instructions that encourage the adoption of 404 compliance practices. - Publish progress reports of each subsidiary's progress toward 404 implementation. - Put drivers for 404 implementation in place. - Direct 404 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.

Figure 9.8.2 CIO Tactics for Implementing SoX Compliance

- **Mobilization:** the action of organizing and encouraging a group of people to take collective action in pursuit of a particular objective

71

Tactic	Definition	Examples of Activities
Standardization	Negotiate agreements between organizational members to facilitate the SoX implementation.	- Use mandatory controls, often embedded within the technology, to which users must comply. - Indicate formal levels of compliance or variance from prescribed controls. - Establish standards of control throughout the organization. - Create an overarching corporate compliance architecture .
Subsidy	Fund implementers' costs during the SoX implementation and users' costs during its deployment and use.	- Centralize template development. - Develop web-based resources. - Train IT staff to implementing 404. - Fund short-term skill gaps. - Track implementation. - Target funds during implementation for specific IT-related 404 goals.

Figure 9.8.3 CIO Tactics for Implementing SoX Compliance

72

IS and the Implementation of SoX Act Compliance

73

- 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 (백지 위임장, 전권 위임) by their CEOs to implement SoX compliance can employ compelling (**convincing**) activities, such as subsidy, standardization, and innovation directives.
- Those CIOs can establish standards and enforce their compliance, creating an overarching corporate compliance architecture.

IS and the Implementation of SoX Act Compliance

74

- 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 (provide)** 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 CEO 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.