Module: INFORMATION TECHNOLOGY MANAGEMENT (IT Management)

مقياس: إدارة تكنولوجية المعلومات

Lecture Handout
For Third Year Student Licence

Speciality: Management

MERAD BOUDIA Mohamed Djamil
Maitre de Conférences Classe A

Intended for third-year Licence students specializing in Management within the Faculty of Economics, Business and Management

TABLE OF CONTENTS

INTRODUCTION

CHAPTER 1 INTRODUCTION TO INFORMATION TECHNOLOGY MANAGEMENT (IT MANAGEMENT)

1. Definition of Information Technology Management (ITM) 6

2. The Role of IT Management in Modern Organizations............................ 7
2.1. Strategic Alignment..7
2.2. Operational Efficiency...7
2.3. Data and Decision Support..8
2.4. Risk Management and Cybersecurity..9
2.5. Innovation and Agility..10
2.6. Customer Engagement and Experience...10

3. Historical Evolution of IT Management 10
3.1. Data Processing Era (1950s–1960s)..14
3.1.1. Mainframe Computers...16
3.1.2. Batch Processing 16
3.1.3. Punched Cards and Magnetic Tapes 16
3.1.4. Limited Interactivity..16
3.2. Management Information Systems (MIS) Era (1970s–1980s)........................17
3.2.1. Technological Context 18
3.2.2. Management Focus 18
3.2.3. Organizational Role: Emergence of the CIO 18
3.3. Strategic Information Systems (SIS) Era (1980s–1990s).................................19
3.3.1. Technological Context: PCs, Client-Server Architecture, ERP Systems.....19
3.3.2. Management Focus: IT as a Source of Competitive Advantage 19
3.3.3. Organizational Role: CIO as Strategic Partner 20
3.4. Internet and E-Business Era (Late 1990s–Early 2000s)..................................20
3.4.1. Technological Context 20
3.4.2. Digital Transformation and Customer-Centric IT.................................21
3.4.3. Organizational Role: IT Drives Innovation and Agility...........................21
3.5. Cloud, Mobile, and Big Data Era (Mid-2000s–2010s) 21
3.5.1. Cloud Computing, Mobile Apps, Social Media, Analytics.........................22
3.5.2. Agility, Scalability, and Data-Driven Decisions....................................23
3.6. Digital Transformation and AI Era (2020s–Present)......................................23
3.6.1. AI, IoT, Blockchain, Quantum, and Edge Computing...............................24
3.6.2. Digital Transformation, Ethical Data Use, and Cybersecurity....................25
3.6.3. IT as Driver of Innovation and Corporate Sustainability..........................25

4. Technology as a Strategic Resource 26
4.1. Strategic Alignment with Business Goals 26
4.1.1. Bridging the gap between technical teams and business leaders 26
4.1.2. Supporting decision-making through data analytics and business intelligence 26

4.2. Enhancing Operational Efficiency 27
4.2.1. Implementing Enterprise Resource Planning (ERP) systems 27
4.2.2. Automating repetitive and manual tasks 27
4.2.3. Ensuring system integration and data consistency 27
4.3. Managing Digital Transformation 28
4.4. Cybersecurity and Risk Management 28
4.5. Resource Optimization and Cost Control 28
4.6. Supporting Innovation and Competitive Advantage 28
4.7. Facilitating Communication and Collaboration 29
4.8. Ensuring Scalability and Flexibility 29
Conclusion 29

CHAPTER 2: IT INFRASTRUCTURE AND OPERATIONS MANAGEMENT

1. The components of IT infrastructure 32
1.1. Computer hardware platforms 33
1.1.1. Main device categories 33
- ❖ Servers 34
- ❖ Clients 34
- ❖ Mobile devices 35
- ❖ Related hardware 36

1.1.2. Strategic Analysis of Core Information Technology Platforms 37
- ❖ Platform Strategy and Competitive Advantage 38
- ❖ Platform Lock-in and Switching Costs 38
- ❖ Architectural Modularity and Agility 38
- ❖ Ecosystem Effects 38

1.1.3. Role in the ecosystem 38
- ❖ Enabling Market Interoperability and Standards 39
- ❖ Driving Innovation and Strategic Differentiation 39
- ❖ Reducing and Centralizing Enterprise Risk 40

1.1.4. Operating system platforms that run on those devices 40
- ❖ Microsoft Windows Server 40
- ❖ UNIX and UNIX-Based Systems 42
- ❖ Linux Distributions 42

1.1.5. Desktop Operating System Platforms 43
- ❖ Microsoft Windows 43
- ❖ macOS (Apple) 43
- ❖ Linux Desktop Environments 44

1.1.6. Interoperability and Cross-Platform Integration 44
- ❖ Dimensions of Interoperability 44

1.1.7. Enterprise and application software 45
- ❖ Enterprise Resource Planning (ERP) Systems 45
- ❖ CRM systems 46
- ❖ Other core business applications 46

1.2. Data management and storage systems 47
1.2.1. Data management and DBMS software 47
1.2.2. Storage hardware and on-premise infrastructure 47
1.2.3. Cloud storage and storage services 47
1.3. Networking and telecommunications platforms 48
1.3.1. Enterprise networking infrastructure 48

1.3.2. Telecommunications and unified communications 48
1.3.3. Wide-area, remote access, and internet connectivity 48
1.3.4. Integration with security and cloud platforms 49
1.4. Internet platforms 49
1.4.1. Websites and public internet presence 49
1.4.2. Intranets 49
1.4.3. Extranets 49
1.4.4. Enterprise web portals and services 49
1.5. Consulting and system integration services 50
1.5.1. Nature and scope of consulting services 50
1.5.2. System integration and implementation 51
1.5.3. Lifecycle support and maintenance 51
1.5.4. Strategic role in infrastructure evolution 51

2. IT Assets: Hardware, Software, and Networks 52
2.1. IT Assets: Hardware 52
2.2. IT Assets: Software 52
2.3. Network Management 52

3. Cloud computing and data centres 53
3.1. Data centers as physical infrastructure 53
3.2. Cloud computing as virtualized service layer 54
3.3. Relationship between cloud and data centers 54
3.4. Governance, risk, and architectural implications 54

4. **IT Service Management (ITSM)** 55
4.1. Concept and scope of ITSM 55
4.2. Frameworks and best-practice models (ITIL) 55
4.3. ITSM, IT assets, and service quality 55
4.4. Strategic and organizational implications 56

5. **Business Continuity and Disaster Recovery** 56
5.1. Business continuity 56
5.2. Disaster recovery 57
5.3. Integrated BCDR and organizational resilience 57
5.4. Standards, governance, and continuous improvement 57

CHAPTER 3 IT GOVERNANCE AND STRATEGY

1. IT Governance Frameworks (COBIT, ITIL, ISO 27001) 57
1.1. Definition and Scope 58
1.2. Theoretical Foundations 58
1.2.1. Strategic Alignment Model (SAM) 58
1.2.2. Resource-Based View (RBV) 59
1.2.3. Core Assumptions of RBV 59
1.2.4. Types of Resources 59
1.3. Importance and Benefits 60
1.4. Enhanced Decision-Making Through Data and Analytics 60

1.5. Improved Organizational Agility 60
1.6. Optimized Resource Allocation and Value Realization 60
1.7. Greater Stakeholder Engagement and IT Credibility 60
1.8. Empirical Performance Outcomes 61
1.9. Key Components of IT Strategic Planning 61
1.9.1. IT Vision and Mission 61
1.9.2. Environmental Scanning 61
1.9.3. SWOT Analysis for IT 62
1.9.4. IT Roadmap 62
1.9.5. Governance Structures 62
1.9.6. Performance Management 62
1.10. Challenges in Achieving Strategic Alignment through IT Governance Frameworks
1.10.1. The "Siloization" and Cultural Divergence 64
❖ Communication Gaps 65
❖ Cultural Resistance 65
❖ Lack of Native Interoperability 65
❖ The "Checklist" Trap 65
❖ Resource Constraints and Lack of Executive Sponsorship 65
❖ Perceived Bureaucracy vs. Agility 65
❖ Inadequate Skills 65

2. Risk Management in IT 66
2.1. Conceptual Frameworks and Standards 67
2.1.1. Processes and lifecycle 67
2.1.2. Frameworks and standards 67
2.1.3. Relationship to information security and governance 67
2.1.4. ISO 31000: The Enterprise Risk Management Standard 68
❖ Establishing the Context 68
❖ Risk Assessment 68
❖ Risk Treatment 68
2.2. Key Challenges in Effective IT Risk Management 68
2.2.1. Subjectivity in Risk Assessment 68
2.2.2. The Compliance-Centric Trap 68
2.2.3. Lack of Top Management Commitment and Integration 68
2.2.4. Dynamic and Distributed Risk Landscape 69

3. IT Compliance and Regulations 69
3.1. Major Global Regulatory Frameworks 70
3.1.1. Data Privacy Legislation (GDPR, HIPAA, CCPA) 70
3.1.2. Industry-Specific and Financial Standards (PCI DSS, SOX) 70
3.2. Challenges in Achieving IT Regulatory Compliance 71
3.2.1. Regulatory Fragmentation and Overlap 71
❖ Jurisdictional Conflicts 71
❖ Harmonization Complexity 71
3.2.2. Dynamic Technological Change 71
❖ Emerging Technologies 71
❖ Continuous Monitoring Requirement 72
3.2.3. Resource and Cultural Constraints 72
❖ High Compliance Cost. 72

❖ Compliance vs. Security Mindset 72

CHAPTER 4 INNOVATION AND DIGITAL TRANSFORMATION

1. IT, Organizations and Strategic Alignment 73
1.1. Concept of business–IT strategic alignment..73
1.2. Strategic Alignment Model (SAM) 73
1.3. Organizational structure, governance, and IT...74
1.4. IT capabilities as strategic assets 74

2. Strategic Alignment Model (SAM)..74
2.1.Core structure of SAM 74
2.1.1. Four domains...75
❖ Business strategy (external, business)..75
❖ IT (or IS) strategy (external, IT)...75
❖ Organizational infrastructure and processes (internal, business)..........75
❖ IT infrastructure and processes (internal, IT).......................................75
2.2.Alignment perspectives in SAM 76
2.2.1. Strategy Execution perspective 76
2.2.2. Technology Potential perspective 76
2.2.3. Competitive Potential perspective..76
2.2.4. Service Level perspective...77
2.3.Intellectual and social dimensions of alignment 77
2.4.SAM in contemporary research and practice 77
2.3.1. SAM in contemporary research 77
2.3.2. Extensions and critiques of SAM 77
2.3.3. SAM in practice and managerial use 78
2.3.4. Typical figures and visual representations...78
2.3.5. Enhancing Organizational Efficiency through the Strategic Alignment Model 78
2.3.6. Clarifying roles, priorities, and decisions 78
2.3.7. Reducing process and system misfits 78
2.3.8. Guiding targeted alignment paths 79
2.3.9. Supporting continuous coordination in dynamic environments 79
2.3.10. Challenges in Implementing the Strategic Alignment Model............79
2.3.11. Conceptual and measurement difficulties 79
2.3.12. Organizational and cultural barriers 79
2.3.13. Dynamic environments and sustaining alignment 80
2.3.14. Governance and capability constraints 80

3. Information systems strategy and organizational structure..................80
3.1.Definitions and Conceptual Foundations 80
3.2.Information Systems Strategy 80
3.2.1. Definition and core concept..81
3.2.2. Main conceptions in the literature 81
3.2.3. Relationship to strategic information systems planning.........................81
3.2.4. IS strategy in the digital age 81
3.3.Organizational Structure and Design 82
3.3.1. Organizational structure 82
3.3.2. Organizational design...82

3.3.3. Contingency and fit perspectives 82
3.3.4. Information processing and systems 82
3.4. Fit and Congruence in Organization Theory 83
3.4.1. Models Linking IS Strategy and Structure 83
3.4.2. Strategic Alignment Model (SAM) 83
3.4.3. Information Intensity and Value Chain Perspectives 84
3.4.4. Governance and Decision Rights in IS Strategy 84
3.5. Patterns of Alignment and Misalignment 84
3.5.1. Centralized vs. Decentralized IS in Different Structures 84
3.5.2. Structural Contingencies (divisional, matrix, network forms) 85
3.5.3. Consequences of Misalignment 85
3.6. IS Strategy, Digital Transformation, and Structural Change 85
3.6.1. From Automation to Process Redesign and Business Scope Redefinition 86
3.6.2. Platformization, Shared Services, and New Structural Forms 87
3.6.3. Dynamic Alignment in Turbulent Environments 87

4. IT capabilities and competitive advantage 88
4.1. IT capabilities in the resource-based view 88
4.2. IT capability and firm performance 89
4.3. From IT resources to competitive advantage 89
4.4. Mechanisms linking IT capabilities to advantage 89

5. Innovation and Digital Transformation 90
5.1. Role of ITM in driving innovation 90
5.2. Digital transformation frameworks and strategies 90
5.3. Leveraging AI, IoT, and blockchain 90
5.4. Overcoming barriers to technological change 91

CONCLUSION 92

LISTE OF FIGURES

Figure 1.1: Eras in it infrastructure evolution 12
Figure 1.2: Infrastructure evolution........ 13
Figure 1.3: Evolution of Information Systems and IT Management Eras 14
Figure 1.4: Data Processing Era (1950s-1960s)........ 15
Figure 1.5: Data Processing Era (1970s–1980s) 17
Figure 1.6: Strategic Information Era (1980s–1990s)........ 19
Figure 1.7: Digital Transformation and AI Era (2020s–Present)........ 24
Figure 2.1: The IT Infrastructure Ecosystem 32
Figure 2.2: Main Device Categorie in Standard Entrerise IT infrastructure........ 33
Figure 3.1: Strategic Alignment 64
Figure 3.2: Risk Context and Scope in Risk Management Processes........ 66
Figure 4.1: Strategic Alignment Model (SAM) 75
Figure 4.2: Alignment between IS Strategy and Organizational Structure 86
Figure 4.3: SAM-based View of IS Strategy and Organizational Infrastructure 87
Figure 4.4: Dynamic Alignment Loop 88

LISTE OF TABLES

Table 1.1: Primary Categories of Enterprise Servers and Their Deployment........ 34
Table 1.2: Types of Clients 35
Table 1.3: Main Categories of Client Hardware at the End-User Layer........ 35
Table 1.4: Primary Categories of Mobile Computing Devices and Their Enterprise Functions 36
Table 1.5: Categories and Governance Focus of Related Hardware 37
Table 1.6: Major Types of Enterprise Application Platforms and Their Primary Business Focus...46
Table 2.1: Key Takeaways for Practitioners 66
Table 2.2: Major Global Regulatory and Compliance Frameworks Governing IT and Data Assets70

INTRODUCTION

Information technology management is the execution planning and organizing technology processes in an organization where the information technology are consistent with organization vision and mission. Supervising resources (hardware, software, networks and personnel to make sure the most effective service delivery), IT Management plays a vital role of helping organizations harness the power of embedding technology in their business process for better decision making, productivity and more innovation. Cost Optimization[1], identify the right tools and techniques for organization as a whole It.

The Management of Information Technology (ITM) is an essential area of study as it connects technology, business planning, and information systems to enhance organizational operations and make informed decisions. Integration of advanced technologies often poses as a challenge given the immense volumes of data generated daily by modern businesses and organizations[2]. ITM seeks to employ technologies in driving innovation, change, productivity improvement, and ultimately sustaining competitive edge. Primarily, it revolves around scheming, executing, controlling, and evaluating technological infrastructure and information systems in the attainment of organizational objectives.

As the ITM field continues to develop, it becomes apparent that evaluating new emerging technologies, deploying information system placement strategies, and information containing security and privacy stewardship are examples of activities that fall under this discipline. Drawing knowledge from multiple disciplines such as computer science, engineering, business and management makes this field interdisciplinary. Investments on technology made by an organization, if done strategically guided by effective ITM practices are bound to reap rewards in positive measurable returns aligned with the organization's objectives and vision[3].

The evaluation of new technologies, planning the implementation of information systems, and ensuring the protection of data privacy are but a few activities that fall within the scope Information Technology Management. A collage discipline stems from computer science

[1] - Luftman, J. (2015). Assessing Business-IT Alignment Maturity. Communications of the Association for Information Systems, p.45.
[2] - Laudon Kenneth C, Laudon Jane P. (2021), Management Information Systems – Managing the Digital Firm, Seventeenth (17°) edition, Pearson, USA, p.67.
[3] - Ayat, M., & Shafiee, S. (2025). Integrating COBIT 2019 and ISO/IEC 27001 for Strengthening IT Governance and Information Security. Proceeding of the International Conference on Economics, Business, Science, and Technology, p.73.

and engineering, business, as well as management. When practiced correctly, ITM ensures that there is a return on investments in technology and it contributes positively towards the long-term strategic objectives of the organization[1].

In a company setting, technology management is not simply the acquisition of latest gadgets, but rather a holistic view of how technology interfaces with business processes, customers, as well as employees. It also bears in mind risk management because new technologies come with their own sets of uncertainties. ITM practitioners have the responsibility of optimizing risk and opportunity.

The ITM ecosystem is evolving too quickly because of the new focus of data analytics and artificial intelligence, which is changing the importance of decisions made across the enterprise[2]. Enterprises increasingly depend on advanced analytics to derive actionable insights from the huge volumes of data available as well as forecast operational and customer trends. Thus, there has been a greater need for experts in ITM for application of AI, Machine learning and cloud computing technologies[3].

Moreover, the adoption of new technology initiatives has integrated ITM with an increasingly pivotal element of business strategy. These companies intend to shift to a fully automated operations model while embracing new and advanced ways of conducting business, all of which requires a solid framework in technology management[4]. This transformation has created emphasis on the need for agility, adaptability, and continuous learning within ITM.

The field of ITM also includes aspects of cybersecurity as more adversaries are launching cyber attacks and data breaches. ITM specialists have the responsibility of assuring the resilience, security, and compliance of the information systems with the information technology governance framework. This can be done through the adoption of the complete security policy, regular security audits, and employee training programs to avoid the unlawful access of sensitive information.

Collaboration is a central theme in ITM since it presupposes smooth relations between the IT divisions, units of the company, and even outside people[5]. Teamwork and collaboration across functions enables technology to serve the organization and its objectives while enhancing

[1] - Kopperapu, R. (2024). Regulatory Frameworks and Compliance Strategies for Protecting Consumer Data. ResearchGate, p.27
[2] - Ekman P., Dahlin P., Keller C. (2002), Management and Information Technology After Digital Information, Routledge Studies in Innovation, Organization and Technology, New York, USA, p.79
[3] - Ekman P., et al (2002), Op.Cit. p.82.
[4] - De Mari, Guus (2009), Five Years of IT Management Improvement, IOS Press, The Netherland, p188.
[5] - Barton, Robert (2003), Global IT Management, ed. Wiley, London, England, p.57.

the performance of the enterprise. It encourages innovation through many ways of tackling problems[1].

Since businesses now operate in interconnected markets with a variety of technological requirements and regulations, globalization has further broadened the scope of ITM. ITM professionals must implement standardized technology solutions across regions while navigating cultural, economic, and legal differences. In a changing market, this global viewpoint improves an organization's competitiveness and resilience.
For ITM initiatives to be successful, leadership is essential. Leaders need to be forward thinking, have a strong grasp of technology, and be able to motivate teams. Under their direction, technology investments are guaranteed to produce the best outcomes and foster organizational expansion[2].

To put it simply, information and technology management is a strategic function that enables businesses to innovate, adapt, and prosper in a technologically driven world. It calls for a combination of strategic thinking, technical know-how, and a dedication to ongoing development. The field of ITM will continue to play a crucial role in organizational success as technology develops, influencing industries all over the world[3].

[1]- Berebbia C.A (2004), Management Information Systems 2004, Fourth International Conference On Information Systems Incorporating GIS& Remote Sensing, Wessex Institute of Technology, UK, editor WIT press, Southampton Boston, USA, p.17.
[2] - Laudon K.& Laundon Jane P., Op.Cit, p.77
[3] - Laudon K.& Laundon Jane P., Op.Cit, p.89

CHAPTER ONE

Introduction to Information Technology Management (IT Management)

1. **Definition of IT Management**
2. **The Role of IT Management in Modern Organizations**
3. **Historical Evolution of IT Management**
4. **Technology as a Strategic Resource**

Introduction

The way companies handle technology is not just about keeping things running - it now plays a key role in gaining an edge, shifting how scholars think about leadership, structure, and planning[1]. This area, known as tech management, looks at how businesses organize, use, while overseeing digital tools to meet targets reduce risks, yet adapt when changes hit[2]. Making sure tech efforts match company aims, so spending on systems actually drives results instead of drifting off course. One classic idea, called the resource-based view, suggests lasting success comes from tech strengths that are hard to copy, like custom data insights or one-of-a-kind software setups others cannot easily replicate[3] .

The world of IT management gets tricky because tech and how companies work keep bumping into each other. Rolling out big systems - say ERP or CRM - isn't just about coding or servers; instead, it hinges on whether the organization can truly absorb them. These tools need to mesh with how people already do their jobs, what they value, and who holds influence[4]. When leaders ignore human reactions or office politics, employees push back, causing delays or poor results. That’s partly because new software shifts control across teams and changes daily habits, forcing reorganization from the ground up. To stay on track, firms use guides like COBIT - not as rigid rules but as flexible blueprints - to link system data to real business goals while reducing surprises[5].

On top of everything, outside pressures keep pushing IT systems to meet tougher rules. Because there’s no single global standard, companies have to follow lots of different laws - like GDPR for personal data or SOX for finance[6]. That means picking solid security frameworks, say ISO/IEC 27001, not just to tick boxes but to actually handle risks smartly. Big businesses juggling multiple countries face messy overlaps in regulations, which can get pricey and encourage shortcuts focused more on audit results than real threat protection. Experts mostly agree: leaders at the top need to set firm boundaries for risk and tightly link tech plans with company goals so every dollar spent on IT brings clear benefits[7].

---

[1]- Laudon K.& Laundon Jane P., Op.Cit, p.102.
[2]- ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association, p.127.
[3]- Cuenca, L., et al. (2014). The Role of Information Technology in Organizational Strategy. Journal of Business Management, p.45.
[4]- Simon, H. A. (1976). Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization (3rd ed.). Free Press. p.120.
[5]- Ayat et al., Op.cit., p.92.
[6]- Kopperapu, R. (2024). Op. Cit, p.39.
[7]- Tsiu, T., et al. (2024). The Impact of IT Strategic Planning Process on SME Performance: A Systematic Review. MDPI, Journal of Open Innovation, p.114

1. Definition of Information Technology Management (ITM)

Management of Technology and Information (ITM) refers to the strategic and systematic approach to planning, implementing, and overseeing the use of technology and information systems within an organization to achieve its objectives. It combines principles from business management, engineering, and computer science to ensure that technology resources are effectively utilized to enhance productivity, innovation, and competitive advantage.

MTI involves tasks such as selecting and deploying new technologies, managing the lifecycle of IT systems, ensuring cybersecurity, aligning technology strategies with business goals, and fostering innovation. It also includes the management of data and information as critical assets for decision-making, operational efficiency, and organizational growth.

By focusing on both the technological and human aspects, ITM aims to bridge the gap between technology and organizational strategy, enabling sustainable growth in a rapidly evolving digital landscape.

The strategic and methodical approach to organizing, implementing, and monitoring the use of technology and information systems within an organization to accomplish its goals is known as information technology and information management, or ITM. It integrates concepts from computer science, engineering, and business management to guarantee that technological resources are used efficiently to boost competitive advantage, productivity, and innovation. [1]

Choosing and implementing new technologies, overseeing the lifecycle of IT systems, guaranteeing cybersecurity, coordinating technology strategies with business objectives, and encouraging innovation are all part of MTI. It also covers the management of information and data, which are vital resources for organizational development, operational effectiveness, and decision-making. ITM seeks to close the gap between organizational strategy and technology by emphasizing both the human and technological aspects, enabling sustainable growth in a rapidly evolving digital landscape[2].

[1] - Dyché Jill (2015), The New IT: How Technology Leaders Are Enabling Business Strategy in the Digital Age, ed. McGraw-Hill Education, United States, p.26.

[2] - Piccoli, Gabriele (2018), “Information Systems for Managers”, ed. John Wiley & Sons, 4th edition, United States, p.25.

2.The Role of IT Management in Modern Organizations

Since technology is becoming more and more essential to corporate operations, strategy, and innovation, IT management plays a crucial role in contemporary organisations. IT management entails monitoring technology resources, systems, and tactics to make sure they support value creation and organisational objectives[1].

2.1. Strategic Alignment

IT management makes sure that investments in technology complement the organization's overarching plan. Organisations can improve efficiency, customer satisfaction, and competitiveness in the market by coordinating IT initiatives with business goals. In IT management, strategic alignment is the process of coordinating an organization's technology initiatives and resources with its overall business goals in order to improve productivity, creativity, and competitiveness. With this strategy, IT initiatives are guaranteed to directly support the organization's top priorities, including expansion, client satisfaction, and competitive advantage. In order to achieve effective alignment, business executives and IT leaders must work together to develop a shared understanding of objectives and capacities[2].

Frameworks and metrics are frequently used by organisations to assess how well IT strategies accomplish business objectives. Cost reductions, ROI, or performance enhancements are a few examples of these metrics. Additionally, strategic alignment places a strong emphasis on flexibility, which helps businesses incorporate cutting-edge technologies that spur innovation while maintaining sustainability and legal compliance[3].

2.2. Operational Efficiency

It describes an organization's capacity to provide goods or services in the most economical way possible without sacrificing quality. In order to achieve the intended results, it entails streamlining internal procedures, making efficient use of resources, and reducing waste. In any business, operational efficiency is a major factor in determining productivity, profitability, and sustainability[4].

Several areas must be prioritised in order to achieve operational efficiency:

[1] - Ekman P., et al (2002), Op. Cit. p.79
[2] - Barton, Robert (2003), Global IT Management, ed. Wiley, London, England, p.57.
[3] - De Mari, Guus (2009), Five Years of IT Management Improvement, IOS Press, The Netherland, p.188.
[4] - Ekman P., et al, (2002), Op. Cit, p.102.

First, process optimisation makes sure that bottlenecks are addressed, redundant tasks are removed, and workflows are streamlined.

Second, integrating technology—such as data analytics and automation—improves decision-making and cuts down on time spent on manual labour.

Third, resource management entails making the most of the material, financial, and human resources at hand in order to improve results.

Organisations can lower expenses, increase customer satisfaction, and react swiftly to changes in the market by implementing operational efficiency. For instance, just-in-time inventory systems in retail and lean manufacturing techniques in production industries have both been shown to improve operational efficiency. Additionally, using techniques for continuous improvement, such as Kaizen or Six Sigma, guarantees that businesses continuously improve their operations to keep a competitive edge[1].

Adding value is just as important to operational efficiency as reducing expenses. Businesses can attain sustainable growth while lowering operational risks by concentrating on quality, customer satisfaction, and innovation. This strategy is especially important in fast-paced fields where success depends on productivity and flexibility[2].

2.3. Data and Decision Support

Utilising tools, analytics, and systems to help organisations make informed decisions is known as data and decision support. This method is essential in today's corporate settings, where data is a key tool for developing operational and strategic plans. Businesses can improve the accuracy and dependability of their decision-making processes by processing and interpreting complex datasets, finding patterns, and forecasting future trends with the help of decision support systems (DSS) and data analytics platforms[3].

The ability to collect, process, and analyse both structured and unstructured data is fundamental to data and decision support. Organisations can derive actionable insights through technologies like machine learning algorithms, data visualisation software, and business

[1] - Gallaugher, John, Information Systems, A Manager’s Guide to Harnessing Technology, ed. Flatwood, 2014, Boston, USA, p.274.
[2] - Morgan, Tony (2002), Business Rules and Information Systems : Aligning IT with Business Goals, Pearson education, Indianapolis, USA, p.105.
[3]- Narayanan V. K. (2000), “Managing Technology and Innovation for Competitive Advantage”, ed. Prentice Hall, United States, p.62.

intelligence (BI) tools. Dashboards, for instance, offer performance metrics in real time, and predictive analytics aids in predicting consumer and market trends[1].

Data is also used by organisations for risk assessment and scenario planning. Financial records, market data, and operational metrics are just a few of the many data sources that are integrated by a strong decision support system, enabling decision-makers to assess options and foresee possible obstacles. This ability improves strategic agility and lowers uncertainty[2].

Decision support capabilities are further strengthened by the increased focus on big data and advanced analytics. Organisations can effectively manage large datasets, guaranteeing scalability and timely insights, by utilising data lakes, cloud computing, and AI-driven analytics. In the end, data and decision support enable companies to drive innovation, optimise operations, and react to market dynamics[3].

2.4. Risk Management and Cybersecurity

IT managers are essential in defending companies against online attacks. They protect sensitive data and guarantee adherence to legal requirements by putting in place strong security procedures and monitoring systems[4].

Cybersecurity and risk management are essential for shielding businesses from possible dangers that might impair operations, compromise private information, or damage their reputation. Financial, operational, strategic, and technological risks are just a few of the risks that risk management aims to identify, assess, and mitigate. Organisations create plans to reduce the impact of these risks and preserve resilience by evaluating their likelihood and impact[5].

As a subset of risk management, cybersecurity deals with threats that target digital infrastructure, including data, networks, and systems. To stop illegal access, data breaches, and cyberattacks, it entails putting in place safeguards like firewalls, encryption, frequent system updates, and user access controls[6]. Cybersecurity is essential to protecting an organization's digital assets because threats like ransomware, phishing, and distributed denial-of-service (DDoS) attacks are becoming more common.

[1] - Narayanan V. K. (2000), Op. Cit, p.88.
[2] - McKenney, J. L. (1995). Waves of Change: Business Evolution through Information Technology. Harvard Business School Press,USA, p.127.
[3]- Pilorget Lionel, Schell Thomas (2018), IT Management – The art of managing IT based on a solid framework leveraging the company's political ecosystem, ed. Springer Vieweg, Wiesbaden, Germany, p.222.
[4] - De Mari, Guus (2009), Five Years of IT Management Improvement, IOS Press, The Netherland, p.135.
[5] - Aitken, Lain (2003), Value-Driven IT Management, ed. MPG Books Ltd, Bodmin, UK, p.89.
[6]- Brown V. Carol, Sambaumurthy V. (1999), Repositioning the IT Organization to Enable Business Transformation, Pinnanflex Educational Resources, Cincinnati, Ohio, USA, p.97.

A cohesive response to both digital and non-digital threats is ensured by effective risk management, which incorporates cybersecurity initiatives into larger plans. Organisations can create standardised procedures for detecting vulnerabilities, handling incidents, and swiftly recovering by implementing international frameworks like NIST or ISO 27001[1]. Businesses can secure their operations, adhere to regulations, and gain the trust of stakeholders by combining proactive risk identification with strong cybersecurity defences. In a time when people are depending more and more on digital technologies, these initiatives are especially important.

2.5. Innovation and Agility

By incorporating cutting-edge technologies like cloud computing, IoT, and artificial intelligence, IT management promotes an innovative culture. Additionally, it fosters organisational agility, which helps companies quickly adjust to shifting market conditions[2].

2.6. Customer Engagement and Experience

Through responsive support systems, individualised services, and digital platforms, IT management improves customer interactions. Technology used well enhances user experience, encouraging satisfaction and loyalty[3].

3. Historical Evolution of IT Management

The historical evolution of information technology (IT) management reflects a shift from technical support functions to a strategic organizational role. In the 1960s and 1970s, IT management primarily focused on automating administrative tasks through mainframe systems and batch processing[4]. By the 1980s, the rise of personal computers and client-server architectures decentralized IT and required more coordinated management approaches. The 1990s saw the advent of enterprise resource planning (ERP) systems and the internet, prompting firms to align IT with business strategy and integrate operations across global networks[5]. With an emphasis on agility, value creation, and governance, cloud computing, big data, and digital

[1]- Khan, M. Khaled, Zheng, Yan (2005), Managing Corporate Information Systems: Evolution and Maintenance, ed. Idea Group Publishing, Sydney, Australia, p.275.
[2]- Lemberger Pirmin, Batty Marc, Big Data et Machine Learning, Les concepts et les outils de la Science Data, ed. Dunod, 2019, Paris, p.82.
[3]- McKean, David (2012), IT Management, Part II Projects, Programs and Business Change, ed. Bookboon, N-Y, USA, p.79.
[4] - McKenney, J. L. (1995). Op.Cit, p.139.
[5]- Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. IBM Systems Journal, 32(1), p.8.

transformation have advanced IT management's function from cost-center oversight to innovation leadership since the 2000s[1]. This development demonstrates how IT is increasingly acknowledged as a force behind organisational transformation and competitive advantage.

IT management has changed over time from just giving technical support to being a strategic part of the organisation. In the 1960s and 1970s, IT management was mostly about using mainframe systems and batch processing to make administrative tasks easier[2]. By the 1980s, client-server architectures and the rise of personal computers had made IT less centralised and required more coordinated management strategies[3]. The internet and enterprise resource planning (ERP) systems came out in the 1990s. They made businesses work together across international networks and align IT with business strategy[4].

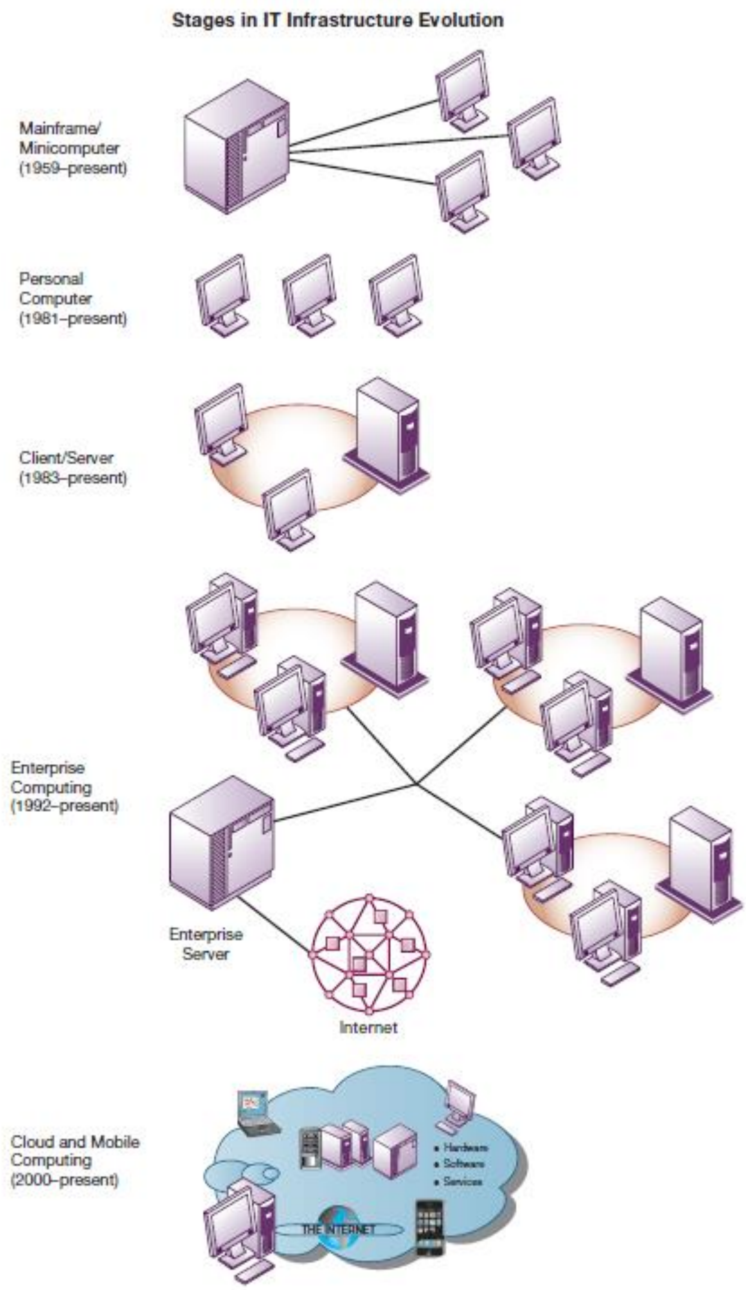
[1]- Swapan Basu (2024), Chapter 14 - Management information system (MIS), Editor(s): Swapan Basu, Plant Intelligent Automation and Digital Transformation, Academic Press, 2024, p.409.

[2]- Melzer, Marvin, Bellingrath-Kimura, Sonoko; Gandorfer, Markus (2023), Commercial farm management information systems - A demand-oriented analysis of functions in practical use, Smart Agricultural Technology, Volume 4, 2023, p.79.

[3] - Applegate, L. M., Austin, R. D., & McFarlan, F. W. (2003). Corporate Information Strategy and Management: Text and Cases (6th ed.). McGraw-Hill, p.107.

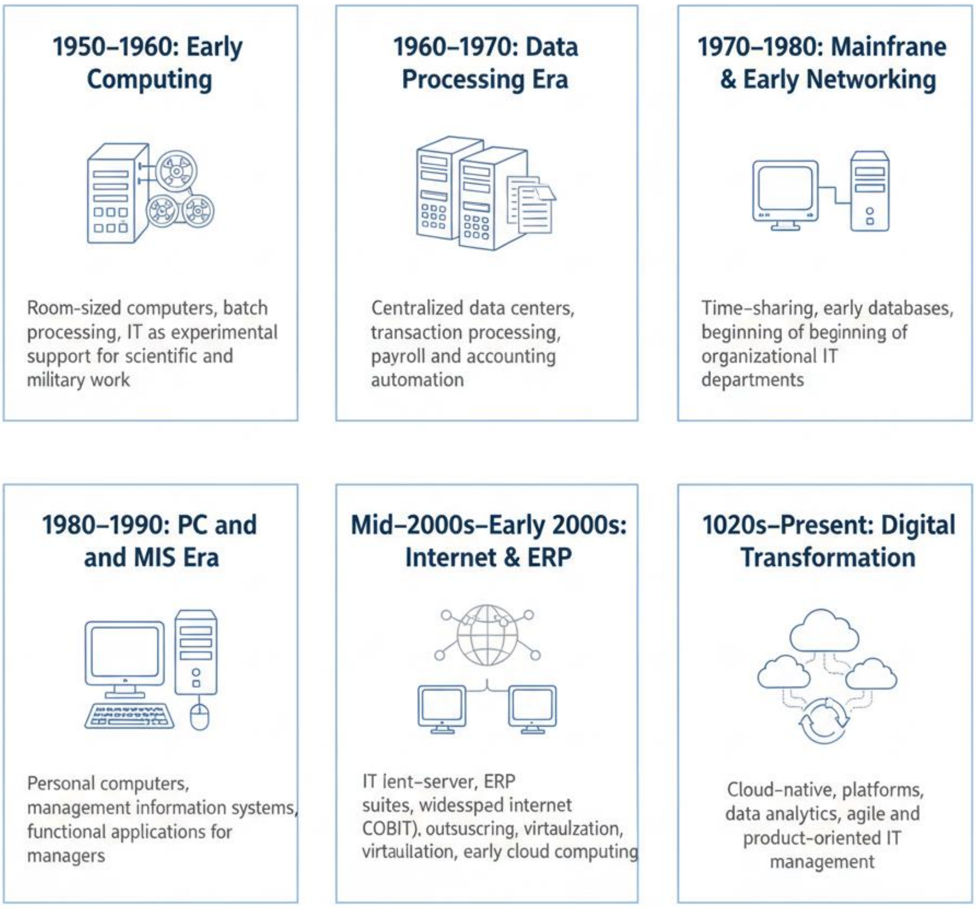
[4]- Henderson J.C. et al, (1993), Op.Cit. p.5.

Figure 1.1: Eras in IT infrastructure evolution



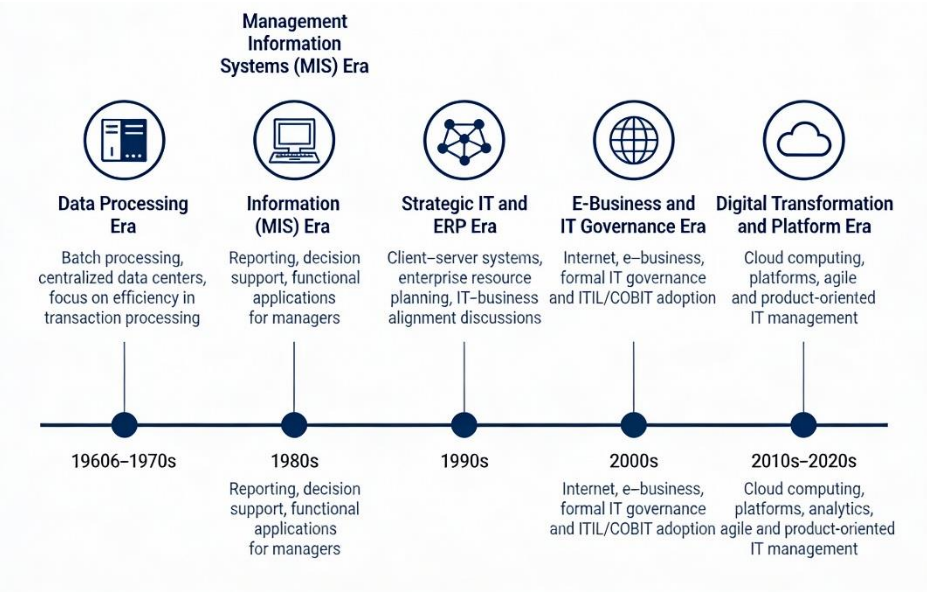
Source : Laudon, K&J (2022), P.168

Figure 1.2: Infrastructure evolution



Source: synthesized by the author based on McKenney (1995), Laudon and Laudon (2021), Applegate et al. (2003), Ceruzzi (2003), and Campbell-Kelly and Aspray (1996).

Figure 1.3: Evolution of Information Systems and IT Management Eras



Source: synthesized by the author based on McKenney (1995), Laudon and Laudon (2021), Applegate et al. (2003), Ceruzzi (2003), and Campbell-Kelly and Aspray (1996).

3.1. Data Processing Era (1950s–1960s)

The Data Processing Era was the first step in the development of IT management. This time, which began in the 1950s and lasted into the 1960s, was marked by the use of large, centralised mainframe computers to automate business tasks that were routine and required a lot of data. At first, companies used IT systems to make tasks like payroll processing, inventory control, billing, and financial accounting more accurate and efficient[1].

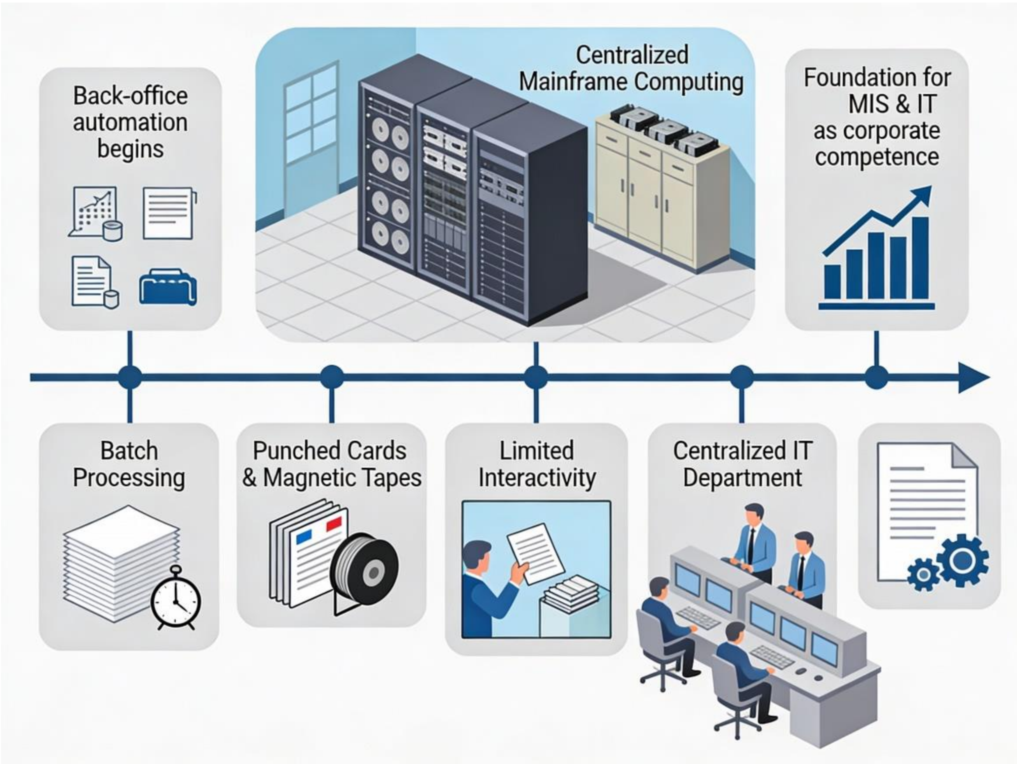
During this time, IT management was very technical and focused on operations. IT managers were in charge of making sure that these expensive and complicated systems worked reliably, handled large amounts of transactions in batch mode, and gave consistent performance. Computing resources were hard to find and expensive, so specialised data processing departments had to control them from one place[2]. This centralisation was necessary to make the best use of resources and keep security and integrity in a place where technology wasn't very flexible.

[1]- Henderson J.C. et al, (1993). Op.Cit, p.6.
[2]- Laudon K, Laudon J. (2021), Op.Cit, p.127.

People mostly thought of IT as a way to help with back-office tasks, but the Data Processing Era set the stage for more advanced uses of information technology in businesses. It brought about formal methods for systems analysis and design, data modelling, and the first types of project management and systems documentation. Over time, these methods would change into the more organised ones used in the development of Management Information Systems (MIS) in later decades[1].

Its importance is found in establishing IT as a corporate competence. Despite its narrow focus, IT management started to evolve as a discipline, with dedicated team members, formalized procedures, and an increased acceptance of the potential for technology to enhance business functions. This era does however represent the defining point in the history of the evolution of IT as a strategic asset.

Figure 1.4: Data Processing Era (1950s-1960s)



Source: synthesized by the author based on McKenney (1995), Laudon and Laudon (2021), Applegate et al. (2003), Ceruzzi (2003), and Campbell-Kelly and Aspray (1996).

[1]- Applegate et al. (2003).Op.Cit, p.116.

3.1.1. Mainframe Computers

The mainframe was the heart of enterprise computing. Early machines such as the IBM 701 (1952), 704 (1954) and the UNIVAC I (1951) were very significant advances in both computational power and reliability[1]. They were built for scientific computation and largescale business data processing, which made it possible for firms to process previously intractable levels of transactions. Mainframes were costly, usually rented rather than bought, and needed their own special facilities and workers, which helped businesses to justify a centralized IT division.

3.1.2. Batch Processing

Batch was the prevailing computational model. It was not an interactive system, instead the jobs to be performed were pre-prepared, bundled into "batches" and were executed sequentially at a chosen time. This had the benefit of being efficient for standardized and repeatable work such as payroll or billing, however it also introduced rigidity and it lacked real-time feedback to users. IT focused on better scheduling, throughput, and error checking to enable the reliable processing of large amounts of data[2].

3.1.3. Punched Cards and Magnetic Tapes

Data input and storage in this period were done via punched cards and magnetic tapes. Punched cards, initially made famous by IBM’s tabulating machines, introduced structured data entry, but necessitated careful manual preparation and handling. Magnetic tape had the advantage of storing more data in a sequential manner for large data files[3]. Collectively, these media provided a means for standardizing workflows, but they limited the systems interactivity and the speed of data access

3.1.4. Limited Interactivity

Computers of that time were <u>not interactive</u> mainframe systems. Users sent jobs to IT staff, who processed them, and waited for output — often hours or days later. And there were no actual terminals or interactive interfaces for users. This dichotomy foregrounded the

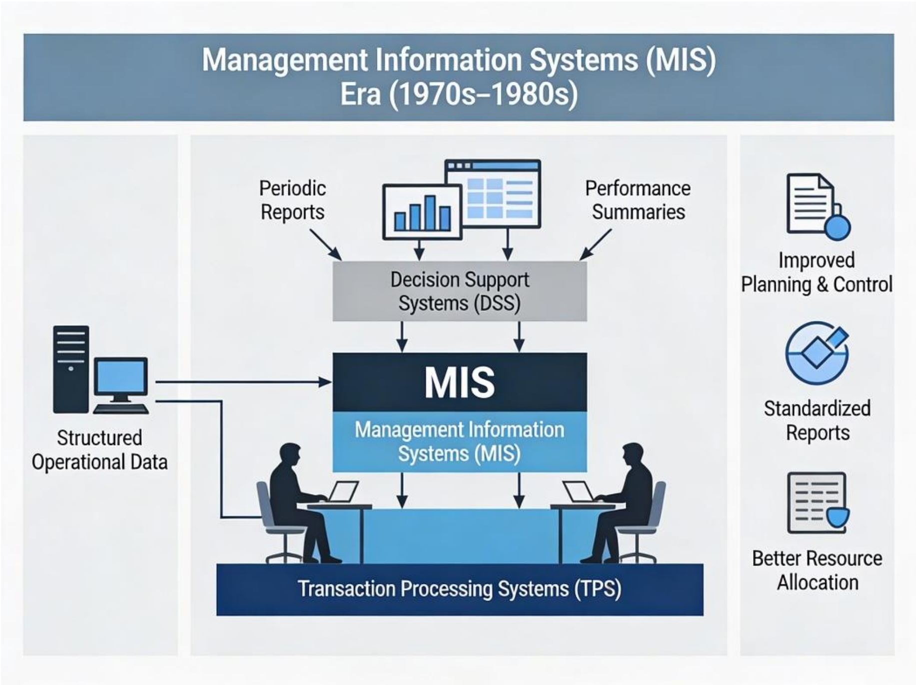
[1]- Ceruzzi, P. E. (2003). A History of Modern Computing (2nd ed.). MIT Press, p.223.
[2]- Laudon K., Laudon J. (2021), Op. Cit., p.128.
[3]- Bughin, J., et al. (2018). Notes from the AI frontier. McKinsey Global Institute, p.77.

gatekeeper role of IT and drove management to focus on scheduling, allocation of resources, and control of operations[1].

3.2. Management Information Systems (MIS) Era (1970s–1980s)

The Management Information Systems (MIS) Era of the 1970s and 1980s marked a critical transition in the role of information technology within organizations. Unlike the Data Processing Era, which focused narrowly on automating routine clerical tasks, the MIS Era emphasized using technology to support managerial decision-making, planning, and control[2]. This period saw IT management evolve from a purely technical function to an essential part of organizational strategy, laying the groundwork for integrating technology with business processes.

Figure 1.5: Data Processing Era (1970s–1980s)



Source: synthesized by the author based on McKenney (1995), Laudon and Laudon (2021), Applegate et al. (2003), Ceruzzi (2003), and Campbell-Kelly and Aspray (1996).

[1]- McKenney, J. L. (1995). Op.Cit, p.146.
[2]- Laudon K., Laudon J. (2021), Op. Cit, p.134.

3.2.1. Technological Context

The technological context of the Management Information Systems (MIS) Era was defined by significant innovations that transformed the way organizations collected, stored, processed, and used information. These technologies shifted IT's role from purely automating transactions to enabling managerial decision-making and strategic planning. While mainframe computers remained the backbone of enterprise IT infrastructure, the 1970s and 1980s saw the proliferation of minicomputers (such as DEC's PDP series). Minicomputers offered lower costs and greater accessibility, allowing departments to develop specialized applications without relying entirely on centralized IT[1]. This shift supported more flexible and decentralized management of computing resources, while mainframes continued to handle large-scale, enterprise-wide data processing.

3.2.2. Management Focus

Centralized IT Departments and Standardization Despite the growing availability of departmental computing, IT management remained highly centralized during this era. Organizations established dedicated IT departments responsible for selecting, developing, and maintaining MIS solutions. This centralization ensured standardization of processes, such as systems development life cycles (SDLC), data management policies, and security protocols2. Formal methodologies became common, with structured analysis and design techniques reducing risk and improving project outcomes. Central IT governance provided consistency in technology strategy, reduced redundancy, and supported integrated reporting across the enterprise.

3.2.3. Organizational Role: Emergence of the CIO

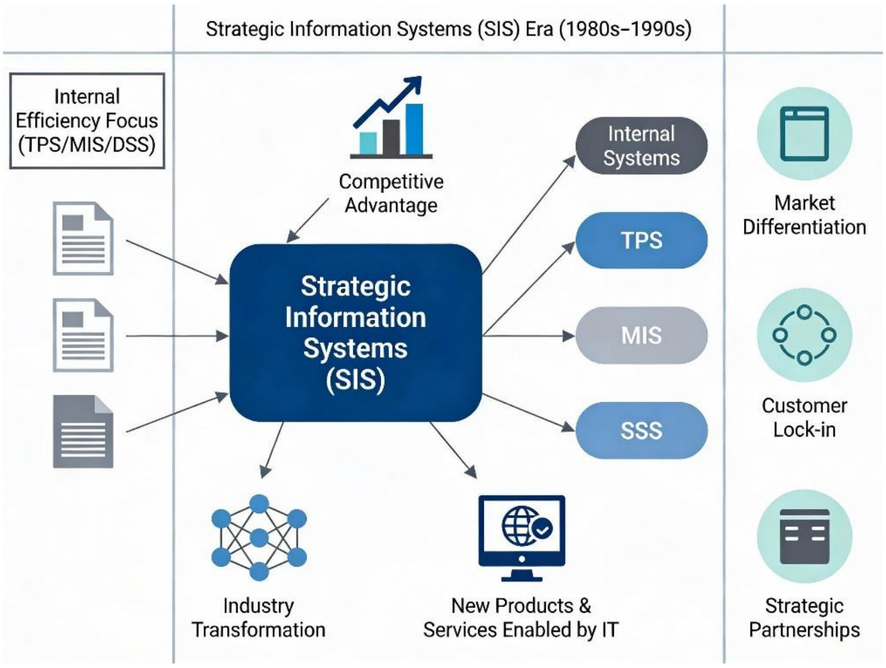
During the MIS Era, the Chief Information Officer (CIO) role began to take shape. As IT became recognized as a critical resource for managing business processes and supporting decision-making, organizations needed senior executives who could bridge technical expertise and business strategy. The CIO was tasked with aligning IT investments with organizational goals, managing growing IT budgets, and ensuring that MIS supported planning, control, and competitive advantage3.

[1]- Ceruzzi, 2003, Op.Cit, p.246.
[2]- Applegate et al. (2003).Op.Cit, p.152.
[3]- Weill, P., & Ross, J. W. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press, p.85.

3.3. Strategic Information Systems (SIS) Era (1980s–1990s)

The Strategic Information Systems (SIS) Era of the 1980s and 1990s marked a transformative shift in the role of IT from operational support to a critical driver of competitive advantage. Organizations began to view IT not just as a cost center but as an enabler of new business strategies, process innovation, and market differentiation. This period established foundational concepts that continue to shape IT management today[1].

Figure 1.6: Strategic Information Era (1980s–1990s)



Source: synthesized by the author based on McKenney (1995), Laudon and Laudon (2021), Applegate et al. (2003), Ceruzzi (2003), and Campbell-Kelly and Aspray (1996).

3.3.1. Technological Context: PCs, Client-Server Architecture, ERP Systems

The technological environment of the SIS Era was defined by several major innovations:

Personal Computers (PCs) became ubiquitous, empowering end-users with direct computing capabilities and decentralizing data access. This democratization of IT reduced dependency on centralized mainframes and enabled more flexible work processes[2].

[1]- Henderson et al, (1993), p.8.
[2]- Ceruzzi, 2003, Op.Cit, p.247.

Client-server architectures replaced monolithic mainframe systems with more modular, distributed systems. Servers provided shared resources, while client applications offered user-friendly interfaces, improving scalability, maintainability, and responsiveness[1].

Enterprise Resource Planning (ERP) systems, such as SAP R/3 and Oracle Applications, emerged to integrate business processes across departments and geographies. ERP systems standardized workflows, improved data consistency, and provided real-time visibility into enterprise operations[2].

3.3.2. Management Focus: IT as a Source of Competitive Advantage

During the SIS Era, IT management shifted from cost reduction to **strategic enablement**. Executives realized that information systems could be designed to support unique business strategies, create barriers to entry, lower costs, differentiate products and services, and lock in customers or suppliers[3]. This new strategic perspective required IT managers to work closely with business leaders to identify opportunities where technology could provide lasting competitive benefits.

3.3.3. Organizational Role: CIO as Strategic Partner

As IT's strategic value grew, the **Chief Information Officer (CIO) role** evolved from technical management to **strategic partnership**. CIOs were expected to participate in executive decision-making, articulate IT's value in business terms, and lead cross-functional initiatives that used technology to transform processes and business models[4]. This period also saw the formalization of IT governance frameworks to align investments with strategic priorities.

3.4. Internet and E-Business Era (Late 1990s–Early 2000s)

The Internet and E-Business Era marked a paradigm shift in how organizations leveraged information technology to create value. The convergence of the World Wide Web, e-commerce platforms, and enterprise integration tools transformed IT from a support function to a catalyst for digital transformation. The era emphasized agility, innovation, and customer-centricity, with IT becoming central to competitive positioning and market responsiveness.

[1]- Laudon K., Laudon J. (2021), Op. Cit., p.134.
[2]- Davenport, T. H. (1998). Putting the enterprise into the enterprise system. Harvard Business Review, 76(4), p.127.
[3] - Porter, M. E. (1996). What is strategy? Harvard Business Review, 74(6), p.61.
[4] - Weill, P., et al (2004), Op. Cit, p.87.

3.4.1. Technological Context: WWW, E-Commerce, and ERP Integration

The late 1990s witnessed the widespread adoption of the internet and web technologies, which enabled organizations to establish direct communication with customers, suppliers, and partners. The World Wide Web (WWW) democratized access to information and facilitated the rise of **e-**commerce platforms (e.g., Amazon, eBay), fundamentally changing how products and services were marketed and delivered.

Meanwhile, Enterprise Resource Planning (ERP) systems, initially internal tools began integrating with external systems through web-enabled architectures. This shift allowed real-time connectivity with supply chains and customer-facing platforms, fostering end-to-end process automation[1]. These technologies served as the backbone for scalable, integrated e-business infrastructure.

3.4.2. Digital Transformation and Customer-Centric IT

Management priorities during this era shifted toward **digital transformation,** redefining organizational processes, business models, and customer engagement through digital technologies. The customer became the focal point of IT strategies, driving the implementation of Customer Relationship Management (CRM) systems and e-business portals that offered personalized services and seamless experiences[2].

Leaders began viewing IT as a strategic asset for enhancing responsiveness**,** reducing transaction costs**,** and enabling innovation. IT investments were evaluated not only in terms of efficiency but also in their capacity to generate new revenue streams and improve customer lifetime value.

3.4.3. Organizational Role: IT Drives Innovation and Agility

During the Internet Era, IT departments transitioned into strategic enablers of business agility. Organizations needed to rapidly adapt to changes in consumer behavior, technology trends, and market competition. The IT function played a central role in creating modular systems, facilitating cross-channel integration, and supporting real-time decision-making.

The rise of e-marketplaces**,** e-procurement**,** and online platforms required IT leaders to coordinate closely with marketing, operations, and logistics. This interdepartmental

[1] - Davenport, (1998), Op. Cit, p.130.

[2]- Chen & Popovich (2003), Understanding customer relationship management (CRM). Business Process Management Journal, 9(5), p.675.

collaboration reinforced the position of IT as a core business function, not a siloed back-office unit.

3.5. Cloud, Mobile, and Big Data Era (Mid-2000s–2010s)

The Cloud, Mobile, and Big Data Era marks a significant shift in how organizations conceive, deploy, and manage information technology. Unlike earlier eras that emphasized internal control and standardization, this phase prioritized agility, scalability, and real-time responsiveness. IT evolved into a dynamic service enabler and innovation platform, empowering organizations to reconfigure their business models and processes in response to unprecedented technological change and market dynamism[1].

3.5.1. Cloud Computing, Mobile Apps, Social Media, Analytics

The technological backdrop of this era was defined by several converging innovations:

- ❖ **Cloud computing** revolutionized IT infrastructure by offering on-demand access to computing resources, storage, and applications via the internet. This model enabled scalability, cost savings, and reduced time-to-market by abstracting infrastructure management[2].
- ❖ **Mobile applications** proliferated with the rise of smartphones, changing how customers interact with firms and enabling "always-on" service delivery. This trend led to the development of mobile-first business strategies[3].
- ❖ **Social media platforms** transformed marketing, customer engagement, and brand management by enabling direct, interactive communication between organizations and consumers[4].
- ❖ **Big Data analytics** emerged as organizations collected massive volumes of structured and unstructured data. Advanced analytics and machine learning techniques turned this data into actionable insights, supporting real-time decision-making and personalization[5].

---

[1] - Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital Business Strategy: Toward a Next Generation of Insights. MIS Quarterly, 37(2), p.475.
[2] - Armbrust et al., (2010), A view of cloud computing. Communications of the ACM, 53(4), p.55.
[3] - West, J., & Mace, M. (2010). Browsing as the killer app: Explaining the rapid success of Apple's iPhone. Telecommunications Policy, 34(5–6), 276.
[4]- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. Business Horizons, 53(1), p.62.
[5]- McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data: The management revolution. Harvard Business Review, 90(10), p.62.

3.5.2. Agility, Scalability, and Data-Driven Decisions

Management priorities evolved from controlling static, monolithic systems to enabling rapid adaptation and innovation. The cloud model facilitated scalable IT architectures that could flex with demand, reducing capital expenditure and improving time-to-market.

Mobile and social technologies forced organizations to adopt customer-centric, omni-channel strategies, demanding real-time responsiveness and personalized experiences. Simultaneously, Big Data analytics shifted management decision-making toward evidence-based, predictive models rather than intuition or static reports[1].

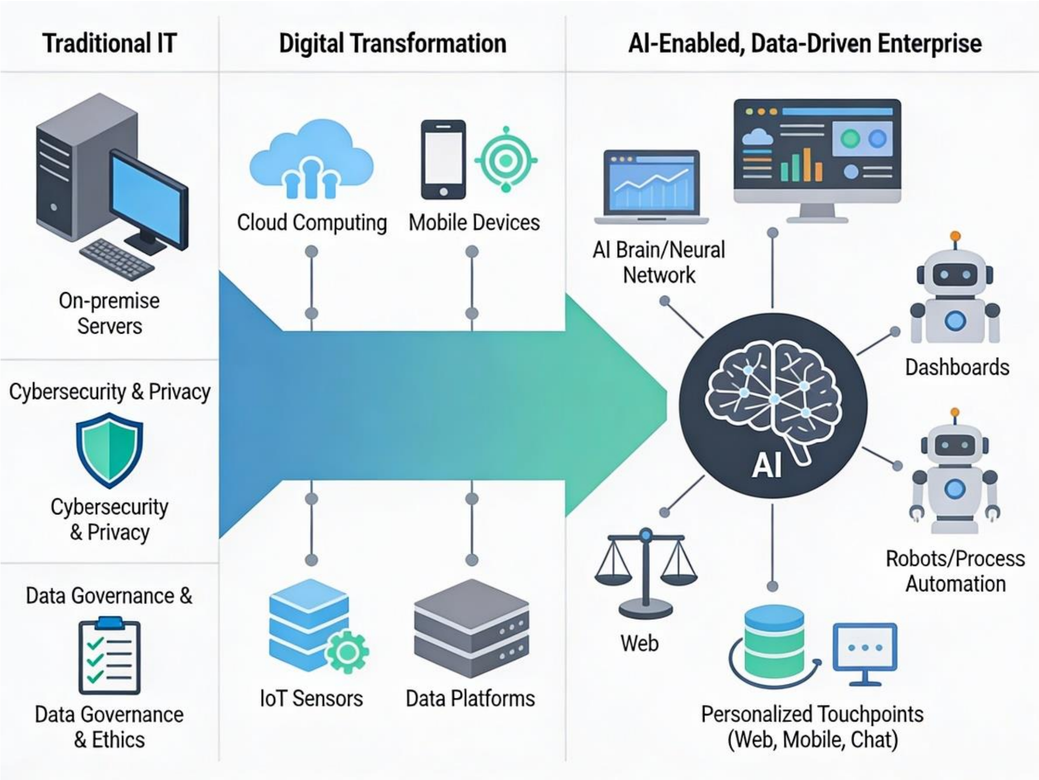
This era required managers to embrace continuous change, balancing experimentation with governance to ensure security, compliance, and quality in an increasingly interconnected environment.

3.6. Digital Transformation and AI Era (2020s–Present)

The Digital Transformation and AI Era represents the most advanced stage in the evolution of information technology management. Unlike earlier eras that focused on efficiency or competitive advantage alone, this phase emphasizes holistic**,** organization-wide transformation integrating advanced technologies**,** ethical frameworks**,** and sustainability goals**.** Organizations increasingly **see** IT as a strategic driver of innovation, resilience, and corporate responsibility[2].

[1]- Chen et al., (2012), Op. Cit, p.676.
[2] - Vial Gregory (2019), Understanding digital transformation: A review and a research agenda, The Journal of Strategic Information Systems, 28 (2), p.120.

Figure 1.7: Digital Transformation and AI Era (2020s–Present)



Source: synthesized by the author based on McKenney (1995), Laudon and Laudon (2021), Applegate et al. (2003), Ceruzzi (2003), and Campbell-Kelly and Aspray (1996).

3.6.1. AI, IoT, Blockchain, Quantum, and Edge Computing: This era is characterized by a convergence of disruptive technologies that are reshaping business models and societal expectations:

- **Artificial Intelligence (AI):** Widespread adoption of machine learning, natural language processing, and generative AI enables personalization, automation, and new product categories[1].
- **Internet of Things (IoT):** Billions of connected devices generate real-time data streams, enabling predictive maintenance, smart cities, and adaptive supply chains[2].

[1] - Bughin et al., (2018), Op. Cit, p.205.
[2] - Atzori et al., (2010), Op. Cit, p.2792.

- **Blockchain:** Distributed ledger technology ensures secure, transparent, tamper-proof transactions, revolutionizing supply chain management, finance, and digital identity[1].
- **Quantum Computing (emerging):** Although not yet mainstream, quantum computing promises transformative breakthroughs in optimization, cryptography, and complex simulations[2].
- **Edge Computing:** Decentralizes data processing closer to devices, reducing latency and supporting time-critical applications in healthcare, manufacturing, and autonomous vehicles[3].

3.6.2. Digital Transformation, Ethical Data Use, and Cybersecurity:

The management agenda has expanded to embrace digital transformation as a core strategic priority. Organizations are rethinking business models, processes, and workforce skills to harness the potential of advanced technologies[4]. Simultaneously, managers face growing pressures to ensure the ethical use of data. Issues such as algorithmic bias, privacy, and consent have moved to the center of IT governance[5]. Cybersecurity has become a critical board-level concern, given the heightened risks of interconnected systems, sophisticated cyberattacks, and regulatory scrutiny[6].

3.6.3. IT as Driver of Innovation and Corporate Sustainability

Its role in organizations has become strategic**,** cross functional, and sustainability-oriented**.** Beyond enabling operational efficiency or market agility, IT is now seen as a catalyst for innovation ecosystems, supporting new products, services, and business models[7].

Organizations also recognize IT's power in supporting environmental, social, and governance (ESG) goals**,** from optimizing energy consumption in data centers to ensuring ethical supply chain traceability via blockchain[8].

[1]- Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications. Telematics and Informatics, 36, p.56.
[2]- Arute et al., (2019), Op. Cit, p.78.
[3]- Shi et al., (2016), Op. Cit, p.256.
[4]- Vial, (2019), Op. Cit, p.139.
[5]- Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. Harvard Data Science Review, p.166.
[6]- Von Solms et al, (2013), Op. Cit, p.100.
[7]- Nambisan et al., (2017), Op. Cit, p.127.
[8]- Loeser et al., (2017), Op. Cit, p.75.

4. Technology as a Strategic Resource

Information Technology Management (ITM) has evolved from a purely operational function into a strategic driver of business transformation. In modern organizations, ITM encompasses planning, implementing, securing, and governing technology assets to support business goals, enable innovation, and ensure sustainability[1].

Modern ITM must manage a complex technological landscape, including cloud computing, AI, IoT, cybersecurity, and data analytics, while aligning technology strategy with dynamic business needs.

4.1. Strategic Alignment with Business Goals

One of the primary and most critical roles of Information Technology Management (ITM) in modern organizations is ensuring strategic alignment, that is, making sure the IT strategy, infrastructure, and projects directly support the organization's overall business goals. Strategic alignment helps maximize the value of IT investments and ensures that technology becomes a true enabler of business success, rather than an isolated operational function.

4.1.1. Bridging the gap between technical teams and business leaders: ITM plays a crucial role as a translator and mediator between technically focused IT professionals and business executives. This ensures that technical solutions are designed to meet real business needs, and that business leaders understand the capabilities, risks, and costs of technology options. This cross-functional communication reduces misunderstandings, accelerates project delivery, and improves the success rate of technology initiatives[2].

4.1.2. Supporting decision-making through data analytics and business intelligence (BI):

ITM enables organizations to move toward evidence-based management by implementing data warehouses, reporting tools, and advanced analytics platforms. Business intelligence systems deliver timely, accurate, and actionable insights that support strategic and operational decision-making. This empowers managers to identify trends, optimize operations, and make informed strategic bets, creating a competitive edge[3].

[1] - Luftman et al., 2004, Op. Cit, p.42.
[2] - Henderson et al, 1993, Op. Cit, p.10.
[3] - Vial G., et al., (2019), Op. Cit, p.145.

Aligning IT investments with organizational objectives: ITM ensures that technology spending is prioritized and justified by its contribution to core organizational goals such as growth, cost reduction, improved customer experience, or innovation. This involves rigorous portfolio management practices, cost-benefit analyses, and governance structures to select, monitor, and evaluate IT projects. By aligning investments with strategy, organizations avoid waste, reduce risk, and ensure resources focus on the highest-value initiatives[1].

4.2. Enhancing Operational Efficiency

A core responsibility of Information Technology Management (ITM) is to enhance operational efficiency by streamlining workflows, optimizing resource usage, and reducing process redundancies. In modern organizations, ITM achieves this by implementing integrated systems and automation tools that improve the speed, accuracy, and coordination of business activities. By doing so, ITM plays a pivotal role in improving productivity, service quality, and cost-effectiveness.

4.2.1. Implementing Enterprise Resource Planning (ERP) systems: ITM introduces and manages ERP systems such as **SAP**, **Oracle**, or **Microsoft Dynamics**, which consolidate diverse business functions—finance, human resources, procurement, inventory—into a unified platform. This integration minimizes duplication, ensures real-time data availability, and enhances cross-departmental collaboration[2]. ERP systems are especially effective in large organizations seeking operational standardization across global units.

4.2.2. Automating repetitive and manual tasks: Routine operations such as invoice processing, payroll, order entry, and customer service can be automated using **workflow management** and **robotic process automation (RPA)** tools. Automation reduces human error, accelerates task completion, and allows employees to focus on more strategic and creative work. According to McKinsey, nearly 45% of work activities could be automated with existing technologies[3].

4.2.3. Ensuring system integration and data consistency: Operational efficiency also depends on the seamless **integration of systems** across departments. ITM manages the design and deployment of **application programming interfaces (APIs)**, middleware, and cloud-based integration platforms to ensure consistent data flow and eliminate information

[1] - Weill & Ross, 2004, Op. Cit, p.92.
[2] - Davenport, 1998, Op. Cit, p.147.
[3] - Chui et al., 2016, Op. Cit, p.247.

silos. This enhances real-time visibility and enables data-driven decision-making across the organization[1].

4.3. Managing Digital Transformation

Digital transformation (DT) has become an imperative rather than an option for modern organizations. It represents a comprehensive, organization-wide change enabled by digital technologies that redefine business models, processes, and customer engagement. Information Technology Management (ITM) is at the center of these transformation efforts—leading strategy, managing change, and integrating technology into all aspects of the organization[2].

Digital transformation is not merely adopting new technologies but involves rethinking how value is created and delivered in a digitally connected world.

4.4. Cybersecurity and Risk Management

In the era of pervasive digital systems, cybersecurity and risk management have become core responsibilities of Information Technology Management (ITM). Modern organizations face escalating threats ranging from ransomware attacks to insider breaches, alongside stringent regulatory requirements for data protection[3].

ITM must design, implement, and continuously improve security policies, procedures, and technologies to safeguard organizational assets**,** ensure regulatory compliance**,** and maintain stakeholder trust**.**

4.5. Resource Optimization and Cost Control

Effective Information Technology Management (ITM) ensures that an organization's IT resources, people, budgets, infrastructure, are used optimally. With technology budgets often representing a significant share of operating costs, ITM must balance delivering value with controlling expenses[4].

4.6. Supporting Innovation and Competitive Advantage

ITM is no longer viewed solely as a support function; it is a strategic enabler of innovation and a source of competitive advantage. Modern organizations rely on ITM to identify, implement, and scale new technologies that reshape products, services, and customer experiences[5].

[1] - Zhao et al., 2021, Op. Cit, p.650.
[2] - Vial, 2019, Op. Cit, p.142.
[3] - Von Solms (2013), Op. Cit, p.102.
[4] - West, J & al., 2010, Op. Cit, p.282.
[5] - Bharadwaj et al., 2013, Op. Cit, p.479.

4.7. Facilitating Communication and Collaboration

Modern organizations are highly interconnected, and effective communication is essential for collaboration across teams, departments, and even continents. ITM facilitates seamless communication and collaboration through technology solutions that support both internal workflows and customer interactions.

4.8. Ensuring Scalability and Flexibility

As organizations grow and adapt to changing markets, they require IT systems that are scalable and flexible. ITM is responsible for designing and managing infrastructures that can expand seamlessly, support new services, and respond quickly to evolving business needs.

Conclusion

A shift began years ago, technology oversight now sits at the core of most modern enterprises, quietly reshaping how work gets structured, executed, and monitored. Rather than just handling gear or software, it involves guiding tech decisions under clear goals, aligning tools with actual needs while respecting limits like budget or risk tolerance. When done well, what was once seen as overhead becomes part of the solution - a quiet force helping firms adapt, invent, stay sharp amid disruption.

Three pieces matter most, infrastructure, software tools, and people, working within structured settings. Networks, machines that store data, computers used daily - all these form a base allowing companies to operate digitally. From there, programs step in, turning raw systems into useful functions like handling payments or studying trends. Communication platforms also fit here, along with interfaces customers use. Without oversight and skilled teams guiding choices, even strong tech can drift off course. Judgment, rules, training, and strategy help match what IT does with what the organization actually needs. Risks get weighed. Compliance isn’t an afterthought - it’s built in.

Began as a behind-the-scenes operator, IT slowly shifted from just keeping systems running to shaping how organizations position themselves. What once centered on streamlining clerical chores evolved - first into feeding reports, then supporting choices, later fueling competitive moves. Step by step, tools meant for routine calculations grew into frameworks influencing leadership decisions. As tech advanced, its presence seeped deeper, turning infrastructure into a quiet force in strategy. Now, platforms driven by machine learning aren't add-ons - they're interwoven with business direction. This shift didn't happen overnight; it reflected an accumulating insight: data and systems now define what companies can become.

These days, IT management sits where tech meets strategy and oversight. Handling more complex setups - like mixed cloud systems, constant network access, rising cyber risks, plus tight privacy rules - is now routine. Still, there's pressure to enable quick adaptation and fresh ideas, especially when rolling out digital tools or experimenting with new ways to do business, sometimes alongside outside partners. Thinking in terms of full lifecycles has become central: starting from design, moving through buying decisions, setup, daily use, all the way to decommissioning gear responsibly without overspending.

Today's tech landscape ties closely to shifts in how organizations operate, make choices based on data, and evolve internally. Leading IT well means working alongside business units, steering change - keeping systems stable while helping define broader goals. With digital tools woven into nearly every part of company operations, understanding core IT management ideas matters more than ever. This knowledge supports those guiding decisions, shaping policy, or navigating careers where digital potential must be balanced with responsibility and real-world consequences.

CHAPTER TWO

IT Infrastructure and Operations Management

1. **The components of IT infrastructure**
2. **IT Assets : Hardware, Software and Networks**
3. **Cloud computing and data centres**
4. **IT Service Management (ITSM)**
5. **Business Continuity and Disaster Recovery**

Introduction

Integrated control of IT setups means overseeing hardware, software, and networks together - so every part helps reach company aims. Rather than handling layers apart, I&O units (Input/Output units) use a full-span method linking tech output to business impact, risk levels, and regulatory needs[1]. Physical gear involves servers, storage tools, desktops, handheld gadgets, plus networking boxes placed locally, in shared centers, or out at remote spots. Good oversight includes forecasting usage demands, tracking device lifespans, managing inventory details, cutting power waste - and watching activity early to reduce breakdown risks. Software acts as a digital framework supporting company operations alongside individual efficiency. This includes OS (Operating System) platforms combined with virtual environments, background services, plus control and tracking utilities including resource planners or customer relationship managers. Connectivity management ensures stable, protected links among people, programs, and information stores. Core components involve hardware units such as signal directors, port hubs, Wi-Fi transmitters, together with standardized transmission rules.

Today’s setups rely more on software-defined networking alongside network function virtualization, enabling flexible control and smoother automation[2].

Security plus compliance are built into every level of infrastructure. Identity controls along with access systems work together with encryption to strengthen defenses. Endpoint protection combined with regular scans help catch weaknesses early. Monitoring tools link directly to operations workflows instead of running separately. These layers interact tightly, cutting risks while meeting legal standards.

Operations management brings in procedures and oversight to operate systems efficiently, covering areas like incidents, problems, changes, resources, and performance, as described by ITIL (Information Technology Infrastructure Library). Because of automation, monitoring tools, and AIOps (Artificial Intelligence Opetations) solutions, teams gain data insights which enable early issue detection, quicker fixes, or even automatic recovery[3].

As cloud and hybrid systems grow, companies handle tasks in private data centers or through public clouds, also using edge sites.

---

[1] - Gartner (2023). IT Infrastructure and Operations Management Market Guide, P.222.
[2] - Gartner (2022). Hype Cycle for IT Infrastructure and Operations, 2022, P.171.
[3] - Greer, M., & Florwick, J. (2021). IT Infrastructure & Operations: Managing in a Hybrid and Multi-Cloud World. O’Reilly Media, p.87.

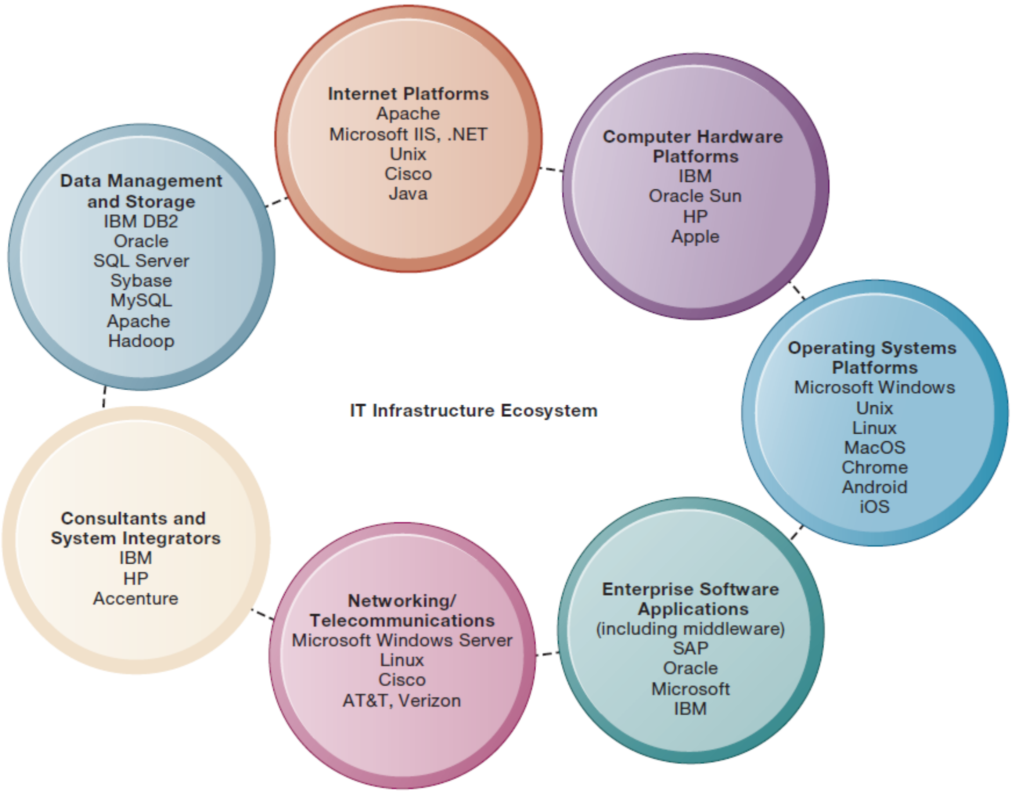
Single oversight, shared rules, or infrastructure coded once support steady performance, lower expenses, yet improve reliability on diverse systems[1].

Overall, combining IT systems and operations helps provide stable, safe, low-cost digital solutions - these support growth while improving market position through better efficiency.

1. The components of IT infrastructure

IT infrastructure today is composed of seven major components[2]. These components constitute investments that must be coordinated with one another to provide the firm with a coherent infrastructure.

Figure 2.1: The IT Infrastructure Ecosystem



Source: Laudon K., Laudon J. (2021), p.177

[1] - Axelos (2019). ITIL 4: Create, Deliver and Support. TSO, p.27.
[2] - Laudon K., Laudon J. (2021), Op. Cit., p.135.

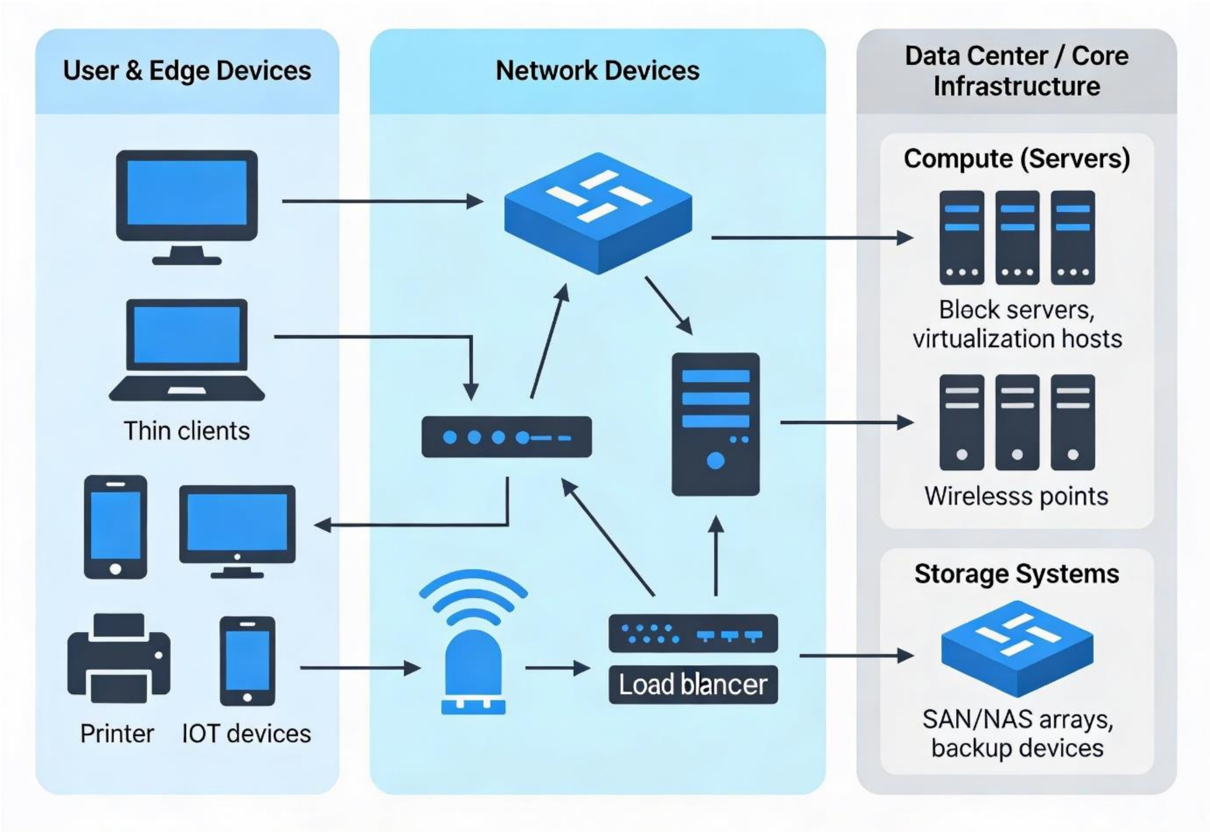
1.1. Computer hardware platforms

Platforms in computer hardware are physical devices that deliver processing power and access for users to the firm's IT architecture. The balls are all the systems that execute the applications, hold the data, and enable user interaction with the information systems.

1.1.1. Main device categories

Client machines include desktops, laptops, tablets, cell phones, and smartphones that people use to connect to the app and data over the network. A server allows the sharing of computing resources and services; it can host a database, enterprise application, web service and VM. Mainframe computers, or mainframes, are powerful centralized machines used in big organizations to process large volumes of transactions.

Figure 2.2: Main Device Categorie in Standard Entrerise IT infrastructure



Source: Adapted from Laudon&Laudon (2007), ISACA (2018) and Tsiu et. (2024)

Servers, clients, mobile devices, and related hardware together form the physical foundation of an organization's IT environment. Each category plays a distinct role in how users access, process, and store information.

❖ **Servers**

Servers are devices on a network that are capable of providing shared resources, data and application to many users. Servers are typically designed to run on specialized server operating systems, have multiple processors or cores, large amounts of memory, and redundant components (power supply units, disks, network interfaces) to ensure high availability. Some examples are file servers, database servers, application servers, web servers, and virtualisation hosts.

Table 1.1: Primary Categories of Enterprise Servers and Their Deployment

Category	**Description**	**Key Characteristic & Deployment**	**Role in Architecture**
Physical Servers	Dedicated, on-premises hardware housed in data centers.	**Form Factors:** Rack (standardized width/height), Blade (modular, high-density chassis), Tower.	Hosts operating systems and hypervisors; provides raw compute power and I/O resources.
Virtual Servers (Virtual Machines - VMs)	Software-defined servers running on a physical host via a **Hypervisor**.	**Deployment:** Highly flexible, rapid provisioning, efficient hardware utilization.	Runs applications and operating systems; provides isolation and resource sharing on a single physical machine.
Cloud Servers (IaaS Instances)	Virtual servers provided by a public cloud vendor (e.g., AWS EC2, Azure VMs).	**Deployment:** On-demand, pay-as-you-go, scalable resources accessible via the internet.	Offers scalable, resilient compute power without the need for on-premises infrastructure management.
Containerization (Microservices Host)	Lightweight, portable software packages that bundle application code and all dependencies.	**Deployment:** Utilizes container runtimes (e.g., Docker) and orchestrators (e.g., Kubernetes).	Focuses on running *applications* rather than entire operating systems, maximizing agility and resource density.

Source **:** Tsiu et al. (2024), p.7

❖ **Clients**

People use client applications on endpoint devices to access the services that servers provide. People often use laptops and desktop computers, which consist of productivity and client operating systems and local apps. Thin clients, also known as virtual desktop terminals, transfer most computational tasks to servers or other cloud platforms. They mainly support the input/output and display functions. Thus, their management is easier and security is significantly improved.

Table 1.2: Types of Clients

Client Type	Description	Processing Capability	Example
Thin Client	Performs minimal processing locally; primarily relies on the server for application execution and data storage.	Low—mostly handles I/O and display.	Virtual Desktop Infrastructure (VDI) terminal, older network computers.
Thick (or Fat) Client	Performs significant application processing locally; only uses the server for data storage and centralized services.	High—runs the majority of the application code.	Desktop email application (like Outlook) that downloads and processes emails locally.
Zero Client	A specialized form of thin client with no local operating system or storage; it simply provides a connection to a remote host.	None—strictly a communication endpoint.	Specialized hardware used for VDI environments.

Source: ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association.

Table 1.3.: Main Categories of Client Hardware at the End-User Layer

Category	Description	Key Characteristic & Deployment	Example Devices
Traditional Clients	Stationary or semi-portable computers designed for resource-intensive, general business tasks.	**Low Mobility;** use full desktop OS and require stable power/network connections (wired or high-power Wi-Fi).	Desktop PCs, Workstations, High-end Laptops, Thin Clients/VDI terminals.
Mobile Computing Devices	Highly portable, battery-powered devices optimized for communication, collaboration, and remote access.	**High Mobility;** managed via **Mobile Device Management (MDM)**; rely primarily on wireless (Wi-Fi/Cellular) connectivity.	Smartphones, Tablets, Wearables (e.g., smartwatches), Convertible Laptops.
Peripheral and I/O Hardware	Devices necessary for human-computer interaction, data capture, and external data output.	**Attached Devices;** convert real-world inputs into digital data and vice-versa.	Printers, Scanners, Keyboards, Mice, Specialized biometric readers, Webcams.
Embedded/IoT Clients	Specialized, often resource-constrained devices designed for automated data collection, sensing, or control tasks.	**Automation/Sensing Focus;** often use low-power networks (e.g., Bluetooth LE, LoRa); managed via specialized IoT platforms.	Smart sensors, Point-of-Sale (POS) terminals, Industrial controllers, Digital signage systems.

Source: Laudon (2024), ISACA (2018)

❖ Mobile devices

Smartphones and tablets allow clients to access a network while not in the office at any time and place. They depend on wireless networks and mobile operating systems and usually use dedicated mobile apps or web interfaces to connect with enterprise systems[1]. Mobile device management, or MDM, is a system that manages corporate data on mobile devices, often those the user owns personally.

Table 1.4 : Primary Categories of Mobile Computing Devices and Their Enterprise Functions

Category	Description	Key Characteristic	Example Enterprise Functions
Smartphones	Full-featured cellular phones with advanced computing capabilities and versatile operating systems.	**High Mobility & Connectivity;** Managed by **MDM** (Mobile Device Management); primary tool for communication and remote work.	Email, instant collaboration, customer relationship management (CRM) access, field service documentation.
Tablets	Larger-screen, thin, and portable devices optimized for content consumption, presentation, and limited data entry.	**Balanced Portability & Screen Size;** Often used as a substitution for laptops in specific roles.	Inventory management (in warehousing), patient bedside data entry (in healthcare), interactive sales presentations.
Wearable Devices	Small, personal computing devices worn on the body, primarily used for data collection, alerts, and notifications.	**Ambient Computing;** Collects biometric and environmental data; low power consumption.	Health monitoring, hands-free work instructions, quick alerts for IT operations staff.
Ruggedized Devices	Specialized mobile devices built to withstand harsh environments (e.g., extreme temperatures, dust, drops).	**Durability & Specific I/O;** Custom-built for industry-specific tasks (e.g., barcode scanning, RFID reading).	Logistics and supply chain tracking, construction site management, military or public safety operations.

Source: ISACA (2018)

❖ Related hardware

Peripherals and infrastructure elements that support these primary device types are referred to as related hardware. Monitors, keyboards, printers, scanners, docking stations, external storage used with clients, racks, power distribution units, cooling equipment, and backup devices situated alongside servers in data centres are all included in this[2]. Servers,

[1] - Kappelman, L., McLean, E., Johnson, V., & Torres, R. (2019). The 2018 SIM IT Issues and Trends Study. MIS Quarterly Executive, 18(1), p.57.

[2] - Karahanna, E., & Preston, D. S. (2013). The Effect of Social Capital of the Relationship Between the CIO and Top Management Team on Firm Performance. Journal of Management Information Systems, p.18.

clients, and mobile gateways are physically connected into a cohesive infrastructure by network interface cards, Wi-Fi access points, and cabling.

To ensure that users have dependable, safe, and effective access to apps and data throughout the company, all hardware components must be selected, set up, and maintained as an integrated platform.

Table 1.5: Categories and Governance Focus of Related Hardware

Hardware Category	Primary Function	Example Devices	Role in IT Infrastructure
Input Devices	Captures data and instructions from the user or the environment and sends them to the computer.	Keyboards, Mice, Scanners, Microphones, Webcams, Touchpads, Barcode Readers.	Translates human action or external data into binary signals for processing.
Output Devices	Presents processed data and information from the computer to the user in a usable format.	Monitors (Displays), Printers, Speakers, Plotters.	Renders processed digital information into visual, auditory, or physical form.
Storage Peripherals	External devices used for saving and retrieving data temporarily or for backup purposes.	External Hard Drives (HDD/SSD), USB Flash Drives, Optical Drives (CD/DVD/Blu-ray).	Provides portable or offline storage capacity outside of the primary server/cloud infrastructure.
Interface Hardware	Components that manage the communication link between the client and the network or other devices.	Network Interface Cards (NICs), Modems, Hubs/Switches (at the edge/desk level), Bluetooth Adapters.	Facilitates physical and data-link layer connections (wired or wireless).

Source: Laudon (2007)

All of these hardware elements must be selected, configured, and managed as an integrated platform so that users experience reliable, secure, and performant access to applications and data across the organization.

1.1.2. Strategic Analysis of Core Information Technology Platforms

Modern servers often use industry-standard processors (for example, from major chip producers) and can be deployed as blade servers in racks to save space and power.

Leading hardware vendors supply integrated server, storage, and client platforms that form the backbone of enterprise computing environments[1].

The strategic analysis of core Information Technology (IT) platforms and the surrounding vendor ecosystem is a critical function within contemporary strategic management,

[1] - Leego, E., & Bider, I. (2023). Aligning ISO 27001 with Business Objectives: A governance perspective. Journal of Systems and Software, p.137.

directly influencing a firm's resource allocation, operational agility, and long-term competitive positioning[1]. This analysis extends the traditional focus on internal resources to encompass the external market forces and vendor capabilities that shape a firm's technological potential.

- **Platform Strategy and Competitive Advantage**

An IT platform is defined as the operating system, hardware architecture, and core middleware on top of which all other business applications are built[2].

- **Platform Lock-in and Switching Costs**

A major concern involves risk of dependency on one supplier - using a closed system (like a single cloud service or large ERP setup) often leads to expensive, time-consuming shifts later[3]. Instead of focusing only on tight integration from niche platforms, firms should weigh this against future adaptability through open, mixed, or cross-system approaches

- **Architectural Modularity and Agility**

Modern strategy favors platforms made of separate parts, like microservices or containers that can be swapped fast. Because these pieces work independently, companies update them swiftly when markets shift. Instead of overhauling whole setups, firms adjust only what is needed. This independence helps adopt top-performing tools smoothly. As a result, organizations respond faster to change without major downtime[4].

- **Ecosystem Effects**

The worth of a platform isn't only about built-in functions - it's tied to how active and large its surrounding environment is, such as outside creators, accessible software, or trained users. Evaluation should look into how strong and stable this outer system really is.[5]

1.1.3. Role in the ecosystem

Computer hardware needs to work well with OSs as well as network setups so that everything fits together properly within an IT environment

Choices in equipment size, uniformity, or upkeep shape how well systems run, stay stable, manage expenses, or use power within a tech-driven company.

---

[1] - Tsiu et al., 2024, Op. Cit, p.124.
[2] - Laudon K., Laudon J. (2021), Op. Cit., p.167.
[3] - Shapiro et al, 1999, Op. Cit, p.79.
[4] - Rizal, A., et al. (2025). Challenges in Harmonizing IT Governance Frameworks: A Case Study of COBIT and ISO Standards. International Journal of Information Management., p.113.
[5] - Tsiu et al., 2024, Op. Cit, p.116.

❖ **Enabling Market Interoperability and Standards**

Platforms plus vendors set the tech rules needed for the system to run and grow, these guidelines make large-scale operations possible since shared frameworks support compatibility while enabling expansion across different services.

- **Standard Bearers**: Major platforms like OS providers or cloud services, set the rules for APIs and communication methods used by apps and data[1]. Because they shape these standards, separate tools made by different companies can work together without issues. Their main job is making sure compatibility happens across devices, programs, and systems from multiple vendors.

- **Facilitators of Network Effects**: A platform's design impacts how strongly network effects emerge. As user numbers grow - alongside participation from external developers the system gains value for everyone involved. This increased utility strengthens market position, which in turn draws additional resources and creative improvements[2].

❖ **Driving Innovation and Strategic Differentiation**

Vendors drive tech progress, supplying tools that help companies outperform rivals.

- **Sources of External R&D**: Companies get outside research help from suppliers when dealing with advanced tech such as artificial intelligence or quantum computing. Because these fields need heavy investment, firms use supplier-led solutions that are ready-to-use, safe, and able to grow[3]. Instead of building core systems themselves, businesses shift focus inward - toward unique advantages. Working this way frees up time and effort for priorities beyond basic infrastructure.

- **Value Chain Acceleration**: Suppliers offer technology - like no-code systems or AIOps - that helps companies build and deliver products faster. Because tasks are automated while software rollouts become easier, businesses adapt more quickly when market conditions shift[4].

---

[1] - Laudon K., Laudon J. (2021), Op. Cit., p.172.
[2] - Shapiro et al, 1999, Op. Cit, p.82.
[3] - Tsiu et al., 2024, Op. Cit, p.124.
[4] - Rizal et al., 2025, Op. Cit, p.114.

❖ **Reducing and Centralizing Enterprise Risk**

In tightly controlled settings, suppliers help spread risk through shared responsibilities, while also supporting oversight efforts across networks.

- **Risk Transfer and Shared Responsibility**: Using an outside provider - particularly for cloud services - means some duties, like safeguarding hardware or managing core systems, shift from company to supplier. In SaaS setups, the provider handles app availability and protection instead; this lets the business concentrate on how it manages information[1].

- **Compliance Enablers:** Platforms need to follow international rules like GDPR or ISO 27001. This adherence helps clients stay compliant by default. Instead of building controls from scratch, firms rely on vendors' approved setups. Because of this, suppliers must offer verified systems along with documentation - proof auditors often demand[2].

1.1.4. Operating system platforms

Operating system (OS) platforms act as a core software level, letting hardware work with apps. Because today's businesses use many device types, like servers, desktops, or smartphones, they need Operating system solutions that are reliable, flexible, so they can handle large, connected tech environments.

❖ **Microsoft Windows Server**

Microsoft Windows Server refers to a series of advanced operating systems built for major computing setups, connected networks, or business-focused tech functions. Created by Microsoft Corp., this system ranks among the top server platforms worldwide, its strong reliability, protection features, alongside broad administrative software integration drive widespread use.

[1] - ISACA, 2018, Op. Cit, p.149.
[2] - Ayat et al, 2025, Op. Cit, p.103.

- ✓ **System Architecture and Core Functionality** includes:
  - NT Kernel design, built for dependable performance.
  - Active Directory Domain Services for centralized identity and policy management.
  - Advanced networking stack, handles domain name queries and allows flexible set-up through code-based control.
  - Process separation along with sandbox methods that helps safe running of applications and services.

- ✓ **Enterprise-Level Capabilities:** Windows Server provides tools suited for business settings, featuring functions that support operations through reliable infrastructure, while enabling management across departments via integrated services; performance scales with demand due to modular design elements working together efficiently:
  - Identity and Security Management
  - Virtualization and Cloud Integration
  - Application and Web Hosting

- ✓ **Manageability and Administrative Tools:** broad range of utilities aimed at smooth IT oversight, built for practical handling:
  - Windows Admin Center, offers a modern web-based plateform for centralized management.
  - PowerShell: A flexible tool for running scripts and helping simplify tough management jobs by using automation.
  - Server Manager: One central interface that lets you set up and check performance of server functions.

- ✓ **Versions and Evolution**: Windows Server changed a lot over time. Key releases were 2003, better security plus updates to Active Directory; then came 2008, followed by 2012, which brought new virtualization tools; after that, 2016 arrived with cloud support built in; later editions like 2019 and 2022 focused on hybrid environments while refining automation features.

- ✓ **Strategic Importance in Organizational IT Infrastructure:** Windows Server remains central to many organizations' IT infrastructure due to:
  - Its compatibility with diverse hardware and enterprise applications
  - Its strong support ecosystem and long-term service (LTS) model.

❖ UNIX and UNIX-Based Systems

UNIX, along with its derivatives, forms a key group of operating systems in computer history. Created during the 1970s at Bell Labs by Ken Thompson and Dennis Ritchie, it brought a design based on separate parts working together, supporting multiple tasks and users at once. This structure influenced later systems used in research, business, and large organizations.

- ✓ **Architectural Principles:** The strength of UNIX lies in its foundational design principles, which emphasize:

  - Modularity: Based on simple tools designed for one job, which work together when linked - boosting adaptability while reducing excess code size by keeping components lean and focused.
  - Mobility: When the coding language emerged, UNIX turned easier to move between systems. Because its core and tools were adaptable, they worked on many hardware types - this helped it spread quickly.
  - UNIX was built for many users at once, right from the start. It lets several people run various tasks at the same time. These operations happen side by side without interference. The system stays stable and secure because of access controls and separated processes.

❖ Linux Distributions

A Linux distribution forms an entire OS around the Linux kernel, linking core libraries with utilities, apps, manager tools, plus setup features - these together deliver working computer environments[1]. Rather than being released as fixed units like closed-source systems, these distros use a flexible structure: parts can be swapped, merged, or adjusted based on particular needs.

Linux remains one of the most influential server platforms, valued for:

[1] - Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). Operating System Concepts (10th ed.). Wiley, p.145.

- Its open-source architecture,
- Cost-effectiveness,
- Modularity,
- Strong performance under heavy workloads.

Major server distros are Red Hat Enterprise Linux (RHEL), also Ubuntu Server, besides SUSE Linux Enterprise Server (SLES).

1.1.5. Desktop Operating System Platforms

Desktop operating systems are the core programs linking hardware with apps on personal computers. These OS platforms manage resources while organizing processes, helping users access functions via visual screens[1]. Instead, they provide tools so people perform work, create content, or exchange messages using intuitive layouts. Their role includes coordinating tasks across devices through responsive design elements and background operations.

❖ **Microsoft Windows**

Microsoft Windows is the most widely used computer operating system, holding around 70–75% of the worldwide market by 2025[2]. Over time, it has gone through multiple design changes; today's version includes:

- Broad support across various programs,
- Enterprise integration,
- Enhanced graphics-based interaction tools, yet simpler visual controls,
- Making it key in commerce, learning, or government operations.

❖ **macOS (Apple)**

macOS is Apple's computer operating system, based on UNIX. This system focuses on close links between devices and programs, creating a streamlined environment tailored specifically for Apple hardware[3]. macOS stands out due to:

- A strong security framework,
- Smooth connection with Apple's devices, also works well across them
- Improved speed when using design or work-related software.

---

[1] - Stallman, R. (2002). Free Software, Free Society: Selected Essays of Richard M. Stallman. GNU Press.
[2] - Poettering, L., & Sievers, K. (2010). System and Service Manager. Red Hat, Inc.
[3] - Levin, J. (2013). Mac OS X and iOS Internals: To the Apple's Core. Wiley.

❖ **Linux Desktop Environments**

Linux desktop environments represent a diverse ecosystem of open-source operating systems sharing the Linux kernel but varying significantly in philosophy, implementation, and target audiences. Unlike Windows and macOS, Linux offers multiple distributions (distros) with different desktop environments, package managers, and configuration approaches[1] (Negus, 2015). Linux-based desktop systems such as Ubuntu, Fedora, and Debian are increasingly adopted due to:

- Open-source flexibility,
- Low resource consumption,
- Customizable interfaces.

1.1.6. Interoperability and Cross-Platform Integration

Interoperability among desktop operating systems means various platforms can share data, run programs, or join centralized control setups - even when their designs differ greatly[2]. When companies use mixed IT setups, smooth interaction across systems plays a key role in shaping tech strategies and improving daily performance. Today's digital workplaces depend on seamless coordination between servers and desktop Oss. This allows:

- Reliable handling of information,
- Consistent security rules across systems
- Reliable login control through a single system
- Seamless work process on multiple gadgets - using one device connects to another through consistent operation.

Server systems usually run business software and data storage, whereas desktop operating environments serve as gateways for people to use those tools. While servers manage heavy workloads, client machines focus on interaction and display tasks.

❖ **Dimensions of Interoperability:** A Dimensions includes:

✓ Technical Interoperability: Protocol-level compatibility and data format exchange
✓ Semantic Interoperability: Consistent interpretation of exchanged information
✓ Organizational Interoperability: Process alignment across platform boundaries

[1] - Luftman, J., & Kempaiah, R. (2007). An Update on Business-IT Alignment: "A Line" Has Been Drawn. MIS Quarterly Executive, 6(3), p.167.
[2] - Melzer et al (2023), Op. Cit, p.88

- ✓ Syntactic Interoperability: Structured data representation compatibility

1.1.7. Enterprise and application software

Business software systems handle key operations company-wide, where ERP and CRM stand out as major types. These platforms gather information and processes into one place, helping teams work together smoothly by using shared data. Instead of scattered records, units rely on consistent inputs to stay aligned. Efficiency improves when actions follow unified workflows rather than isolated efforts.

❖ Enterprise Resource Planning (ERP) Systems

ERP systems are software packages that combine tools to handle key business tasks in one platform. Because they use shared data storage, teams like accounting, hiring, manufacturing, purchasing, and shipping access the same up-to-date details[1].

ERP as Socio-Technical Systems: ERP systems are often seen as blends of social and technical elements. These platforms include tools for management, workflow rules, and adjustable software parts. Instead of just technology, they combine people processes with digital structures. One goal is cutting delays in communication across teams. They also aim to lower errors in transactions between units. Better data accuracy tends to follow from their use. Managers gain access to consolidated reports through them. Insights for daily operations come from built-in analytics. Strategic choices may improve due to reliable inputs[2].

Modular Architecture and Core Components: Core ERP systems usually include finance tracking, cost management, inventory control, manufacturing scheduling, order handling, workforce administration, along with customer engagement tools and reporting features in modern versions[3]. Thanks to a block-based design, firms can roll out functions systematically based on key goals, meanwhile, shared databases ensure uniform records like client details, vendor info, product specs, and workflow rules throughout operations.

ERP Implementation and Organizational Change: ERP systems often require companies to rethink how they work, since standard processes built into the software

[1] - Gartner (2023), Op. Cit, p.229.
[2] - Hendry N. et al (2024), Design and development of a web-based patient management information system, Procedia Computer Science, V.234, 2024, p.1802.
[3] - Ammann J. et al (2022), Op. Cit, p.300.

may clash with current practices. Research shows these projects can boost efficiency, shorten processing times, strengthen oversight, while increasing clarity across departments, yet challenges like complicated setups, employee pushback, or poor fit between tool and workplace remain common hurdles[1].

- **CRM systems**

CRM systems are business tools aimed at handling key customer-facing tasks like sales, marketing, or service throughout the whole customer journey[2]. These platforms gather client information in one place, assist automated outreach efforts, while also offering analysis features - enabling companies to strengthen how they attract, keep, maintain profitable connections.

- **Other core business applications**

Besides ERP and CRM, companies use key tools like supply chain software, HR systems, project tracking programs, or data analysis platforms. These solutions work as a connected network - linking daily operations with customer engagement and insight-driven functions - to support decisions across both strategy and execution[3].

Table 1.6: Major Types of Enterprise Application Platforms and Their Primary Business Focus

Platform type	Primary focus	Key business functions
ERP	Back-office integration	Finance, accounting, procurement, inventory, production, basic HR
CRM	Customer-facing processes	Sales, marketing, customer service and support
SCM	Flow of goods and materials	Demand planning, logistics, warehousing, supplier coordination
HCM/HRM	Workforce management	Recruitment, payroll, talent management, time and attendance
BI/Analytics	Decision support	Reporting, dashboards, advanced analytics on enterprise data

Source: Adapted from industry documentation on ERP, CRM, SCM, HCM, and analytics platforms

[1] - Atzori L. et al (2010), Op. Cit, p.2802.
[2] - Byrd, T. A., et al (2001). An exploratory examination of the relationship between flexible IT infrastructure and competitive advantage. Information & Management, 39(1), p.45.
[3] - Cuenca, L., et al. (2014), Op. Cit, p.52.

1.2. Data management and storage systems

Data management and storage systems constitute the technological and organizational infrastructure through which data is captured, organized, stored, retrieved, and preserved across its lifecycle in an enterprise context[1]. In academic terms, they combine logical mechanisms (such as database management systems) with physical and virtual storage resources (such as disk arrays, storage area networks, and cloud storage services) to ensure that data remains available, consistent, secure, and usable for operational and analytical purposes.

1.2.1. Data management and DBMS software

At the logical level, enterprise data management is typically implemented through Database Management Systems (DBMS), which provide structured models and query mechanisms for defining, manipulating, and controlling access to data. A DBMS abstracts the underlying storage details, enforces integrity constraints and access controls, and supports concurrent, multi-user operations, thereby enabling reliable transaction processing and consistent views of shared data assets[2].

1.2.2. Storage hardware and on-premise infrastructure

Data management depends on underlying storage hardware, including direct-attached storage, network-attached storage, and storage area networks that aggregate disks, solid-state drives, and controllers into resilient, high-performance subsystems. These infrastructures support redundancy, backup, and recovery mechanisms, and are often integrated with data protection and lifecycle management policies to satisfy availability, performance, and compliance requirements in enterprise environments.

1.2.3. Cloud storage and storage services

In contemporary architectures, cloud-based storage services (object, block, and file storage) extend or replace traditional on-premise storage by offering elastic capacity, geographic distribution, and managed durability as part of an outsourced infrastructure model. From an academic perspective, such services can be viewed as virtualized storage layers that decouple logical data management from physical location, raising new questions about latency, governance, data sovereignty, and cost optimization in data-intensive systems.

---

[1] - Kappelman, L., et al (2019). Op. Cit, p20.
[2] - Atzori L. et al (2010), Op. Cit, p.2803.

1.3. Networking and telecommunications platforms

Networking and telecommunications platforms constitute the foundational infrastructure that enables digital connectivity, communication, and data transfer within and beyond organizational boundaries[1]. They encompass the hardware, software, and services that support local, metropolitan, and wide-area networking, as well as voice, video, and data communication with external stakeholders such as customers, partners, and cloud providers.

1.3.1. Enterprise networking infrastructure

Enterprise networking platforms include local area networks (LANs), data center networks, wireless LANs (Wi-Fi), and wide area networks (WANs) that interconnect end-user devices, servers, and application platforms across sites[2]. Core components typically comprise routers, switches, wireless access points, firewalls, and software-defined networking (SDN) controllers that manage routing, segmentation, quality of service, and security policies across the organizational network fabric[3].

1.3.2. Telecommunications and unified communications

Telecommunications platforms provide voice, video, and real-time messaging services via technologies such as IP telephony (VoIP), session initiation protocol (SIP) trunks, and unified communications and collaboration (UC&C) suites. These systems integrate telephony, conferencing, presence, and instant messaging into a converged environment, enabling synchronous and asynchronous communication between internal users and external parties independent of physical location[4].

1.3.3. Wide-area, remote access, and internet connectivity

For inter-site and external connectivity, organizations use WAN technologies such as MPLS, SD-WAN, VPNs, and dedicated internet access to securely connect branch offices, remote workers, partners, and cloud services[5]. These platforms provide encrypted tunnels, traffic optimization, and policy-based routing that ensure reliable, secure data transfer between geographically distributed actors and external service providers[6].

---

[1] - Cuenca, L., et al. (2014), Op. Cit, p.53.
[2] - Bughin, J., et al. (2018), Op. Cit, p.27.
[3] - Bughin, J., et al. (2018), Op. Cit, p.29.
[4] - Atzori L. et al (2010), Op. Cit, p.2803.
[5] - Melzer et al (2023), Op. Cit, p.92.
[6] - Bughin, J., et al. (2018), Op. Cit, p.29.

1.3.4. Integration with security and cloud platforms

Modern networking and telecommunications platforms are tightly integrated with network security controls (for example, next-generation firewalls, secure web gateways, zero-trust network access) and cloud connectivity services (such as direct cloud interconnects and SASE architectures)[1]. This integration enables organizations to enforce consistent security policies, monitor traffic, and optimize performance for both on-premise and cloud-hosted applications, while supporting scalable, flexible connectivity for digital business ecosystems.

1.4. Internet platforms

Internet platforms that support websites, intranets, extranets, and related web services provide the digital environment in which organizations publish content, collaborate internally, and interact securely with external stakeholders[2]. They combine web servers, content management systems, portal frameworks, and integration middleware, often deployed on cloud infrastructure, to deliver browser-based access to information and applications[3].

1.4.1. Websites and public internet presence

Corporate websites are public-facing platforms on the global internet used for branding, marketing, e-commerce, and information dissemination to broad external audiences[4]. Technically, they rely on web servers, domain name services, and often cloud hosting and content delivery networks to ensure scalability, availability, and performance[5] (Krishnamurthy & Wills, 2006).

1.4.2. Intranets

An intranet is a private, internal web platform accessible only to an organization's employees, designed to support communication, collaboration, and access to internal resources[6] (Strother et al., 2012). Modern intranets function as enterprise portals, integrating document management, HR self-service, news, workflows, and links to business applications through a secure, role-based interface[7] (Benbya et al., 2004).

[1] - Kindervag, 2010; Gartner, 2019.
[2] - Holsapple & Sena, 2005; Turban et al., 2018.
[3] - Papazoglou & Van Den Heuvel, 2007.
[4] - Laudon K., Laudon J. (2021), Op. Cit., p.255.
[5] - Efe, A. (2023). A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. Journal of Auditing and Assurance Services, 3(2). P.17.
[6] - Floridi, L. et al (2019), Op. Cit., p.168.
[7]- Henderson, J. C. (1993), Op. Cit., p.12.

1.4.3. Extranets

An extranet extends selected parts of the organization's internal web environment to approved external parties such as suppliers, partners, or key customers via secure, authenticated access[1]. These platforms typically provide B2B portals for order tracking, project collaboration, document exchange, and self-service dashboards, while enforcing granular authorization and encryption over internet connections[2].

1.4.4. Enterprise web portals and services

Enterprise web portals unify multiple websites, intranets, and extranets into a single access point, often built on portal or digital experience platform (DXP) technology[3]. They integrate with back-end systems (ERP, CRM, HRM) and expose functionality through web services and APIs, increasingly using cloud platforms and microservices architectures to support personalization, analytics, and scalable multi-tenant deployments[4].

1.5. Consulting and system integration services

Consulting and system integration services constitute a critical layer in the enterprise IT ecosystem, providing the specialized expertise required to design, implement, integrate, and maintain complex information infrastructures across heterogeneous platforms and organizational units[5]. These services bridge the gap between business strategy and technology by aligning architectures, processes, and governance mechanisms with organizational objectives, regulatory constraints, and industry best practices

1.5.1. Nature and scope of consulting services

IT consulting services support organizations in assessing their current infrastructure maturity, defining target architectures, and developing roadmaps for digital transformation, infrastructure modernization, and sourcing strategies[6]. Consultants typically provide methodological guidance on requirements analysis, solution selection (for example, ERP, cloud platforms, security tools), and IT governance structures, ensuring that technical designs are consistent with business models, risk appetites, and compliance requirements.

---

[1]- Tsiu, T., et al. (2024), Op. Cit, p. 119
[2] - Shapiro, C. (1999), Op. Cit, p. 146.
[3] - Peppard, J. et al. (2004), Op. Cit, p.169.
[4] - Shi, W., et al. (2016), Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), p.640.
[5] - Tallon, P. P., & Pinsonneault, A. (2011). Competing perspectives on the link between strategic information technology alignment and organizational agility: Insights from a mediation model. MIS Quarterly, 35(2), p.482.
[6] - Weill, P.et al (2004), Op. Cit, p. 127.

1.5.2. System integration and implementation

System integration services focus on the technical and organizational integration of disparate applications, data sources, and infrastructure components into a cohesive, interoperable environment. This often involves middleware, APIs, enterprise service buses, and data integration tools, as well as project management, configuration, customization, testing, and migration activities required to deploy large-scale systems such as ERP, CRM, and cloud-based solutions[1].

1.5.3. Lifecycle support and maintenance

After the initial deployment, consulting and integration firms often provide for system lifecycle support, application management, performance tuning, and continuous improvement services[2].These processes include monitoring, incident and change processing, upgrading, and tuning of architectures and processes for maintaining service levels, reliability, and security in dynamic technological and business environments.

1.5.4. Strategic role in infrastructure evolution

Looking at things through a scholarly lens, support from consultants and system integrators acts less like a fix and more like scaffolding - helping firms handle tangled systems while easing the adoption of tools like cloud platforms, microservices, or data analysis methods[3]. Research shows success isn't just about skill in coding or setup; it leans heavily on how well know-how moves across teams, how trust builds in collaborations, and whether goals match up between buyer and vendor - all shaping both immediate results and how sturdy tech setups stay over time[4].

---

[1] - Bofan Song, Rongguang Liang (2024), Integrating Artificial Intelligence with Smartphone-based Imaging for Cancer Detection in vivo, Biosensors and Bioelectronic, p.103.
[2] - Kaplan, A. M., et al (2010), Op. Cit, p. 64.
[3] - Muhammad A., Zainab Riaz, Christophe Cruz (2023), Revolutionizing Management Information Systems with Natural Language Processing for Digital Transformation, Procedia Computer Science, Volume 225, 2023, P.2839.
[4] - Peppard, J., & Ward, J. (2004) Op. Cit, p.172.

2. IT Assets: Hardware, Software, and Networks

Achieving solid results in IT services often ties back to how teams are arranged structure shape whether hardware, software, and networks work together smoothly. Not every setup manages this well; some stumble when linking tech layers to daily operations. When it clicks, though, coordination tends to improve mobility across departments. Efficiency is not automatic; it grows where systems align without friction. Strategic goals gain clearer paths forward if digital tools are not working against each other[1].

2.1. IT Assets: Hardware

Few things matter more than keeping an organization’s machines running, servers, desktops, drives, hubs, or gadgets tucked around corners. Oversight kicks in the moment gear arrives, tagging each piece so nothing slips through cracks later on. Tracking does not stop at labels; it follows lifespan stages, from setup to retirement, adjusting schedules before breakdowns hit. Performance checks happen quietly, feeding data that keeps systems stable without constant oversight. Maintenance is not just fixing, it is avoiding failure by acting early, consistently. Scaling up means adding parts smoothly, never forcing mismatched pieces together. Planning involves power use, how duplicates handle traffic if one fails, even whether tomorrow's tools will plug into today's racks[2].

2.2. IT Assets: Software

Software melts data to the operational level which is to be performed on the hardware. Software includes system software which is operating system (OS), system software, middleware, and business application software. It includes the system for selection, deployment, configuration, software patching, versioning and upgrade, and renewal of software licenses which complies business operations. It also includes software license compliance, version.

2.3. Network Management

Network management involves overseeing the organization’s communication ecosystem that connects different hardware and software systems for the sharing of information both internally and externally. This includes configuring and monitoring the company’s routers, switches, firewalls, wireless access points, and Virtual Private Networks (VPNs).

[1] - Gulzar, Maryam (2023), IT Infrastructure Management: A Digital Services Context, LUT University, Yliopistonkatu 34, 53850 Lappeenranta, Finland, p.127.
[2] - Gartner (2022). Op. Cit, p.202.

The effectiveness of a network is evaluated based on its bandwidth, latency, uptime, and security[1]. Important processes within network management are fault detection, capacity planning, network service supervision (quality of service), as well as enforcement of cybersecurity policies to mitigate and neutralize threats while maintaining uninterrupted network access[2].

3. Cloud computing and data centres

Cloud computing works alongside data centers - both shape how tech resources are built and shared, offering processing power, space for files, along with network links essential for online tools and platforms[3]. Today's studies on digital systems see them as blends of people and technology, allowing flexible access to computing strength, shifting who holds authority when companies rely on outside vendors for support[4].

Due to the exponential growth in demand, technological advancements, and sustainability imperatives, data centres and cloud computing are currently undergoing significant transformation. While cloud computing provides scalable, on-demand virtualised services that are becoming more and more dominant in the market, data centres continue to serve as the physical backbone housing enterprise IT resources[5].

3.1. Data centers as physical infrastructure

Enterprise data centers are specialized facilities that house computing, storage, and networking equipment within controlled environments designed for reliability, security, and energy efficiency[6]. They provide the physical layer for centralized processing and storage, incorporating redundancy in power supply, cooling, and network connectivity, as well as resilience mechanisms aligned with formal availability and disaster-recovery objectives[7].

[1] - Sparrow Elizabeth (2003), Successful IT Sourcing – From Choosing a Provider to Managing the Project, ed. Springer, London, UK.
[2] - Gulzar, 2023), Op. Cit, p.132.
[3] - Melzer et al (2023), Op. Cit, p.95.
[4] - Muhammad Arslan et al (2023), Revolutionizing Management Information Systems with Natural Language Processing for Digital Transformation, Procedia Computer Science, V.225, p.2839.
[5] - Chui et al, 2016, Op. Cit, p. 288
[6] - Chui et al, 2016, Op. Cit, p. 289
[7] - Brightlio. (2025). 215 Data Center Stats (June-2025).

3.2. Cloud computing as virtualized service layer

Cloud computing hides the complexity of physical servers, offering simplified tools that behave like IaaS, PaaS, or SaaS - available online via intuitive portals with usage-based costs[1]. Instead of owning hardware, companies draw from shared pools of capacity, scaling up or down depending on demand while accessing capabilities through widespread connectivity. Resources are reused across users, adapting quickly when needs shift, making it easier to manage workloads without heavy upfront investment[2]. This model tracks consumption closely, turning fixed IT spending into variable expenses tied directly to actual use.

3.3. Relationship between cloud and data centers

Larger public and private cloud setups run across uniformed server hubs spread wide in location managed by companies or specialized vendors[3]. Unlike classic corporate server rooms, built just for one group, cloud centers handle multiple users at once, weaving complex management systems with virtual frameworks that shift computing power around based on who needs it[4].

3.4. Governance, risk, and architectural implications

The shift away from purely on-site servers toward cloud systems brings up real questions about where data lives, how rules are followed, security risks, along with dependency on outside vendors[5]. Lately, studies have pointed to blended setups - mixing private and public clouds, and distributed models like edge or fog computing, helping balance tasks between local facilities and remote platforms without sacrificing speed, compatibility, or reliability[6].

[1] - Wang, T., et al. (2024). A Survey of Major Cybersecurity Compliance Frameworks. Proceedings of the IEEE International Conference on Cyber Security and Resilience, p.25.
[2] - Casino et al (2019), Op. Cit, p. 69
[3] - Alireza Nili, Colin Fidge, Michael Rosemann (2024), Why do project managers underuse Management Information Systems theories in their management of IT projects?, Procedia Computer Science, Volume 239, 2024, P.1580.
[4] - Laudon K., Laudon J. (2021), Op. Cit., p.448.
[5] - Casino et al (2019), Op. Cit, p.79.
[6] - Chui et al, 2016, Op. Cit, p. 292.

4. IT Service Management (ITSM)

A typical take on IT Service Management sees it as how groups organize tasks, workflows, and habits to shape, run, and then refine digital services - always with an eye on what the business or end person actually requires. Unlike setups fixated only on tools or systems, this approach leans into structured methods focused more on shared outcomes, real usability, and slow but steady upgrades instead of juggling tech pieces one by one[1].

4.1. Concept and scope of ITSM

A fresh look at ITSM positions it within broader service management - narrower in scope, yet centered on how organizations handle their tech tools and skilled staff as active offerings. Rather than treating systems or teams in isolation, the focus shifts toward delivering value across departments, whether inside the company or beyond. Planning kicks things off, followed by shaping services, moving them into use, running them day-to-day, then refining over time. These stages are not rigid steps but overlapping phases woven into ongoing practice. Governance plays a quiet but steady role here, ensuring tech efforts do not drift from corporate goals or acceptable levels of risk[2].

4.2. Frameworks and best-practice models (ITIL)

A fresh take on ITSM often begins with what many now consider standard ITIL. This model lays out clear direction for handling incidents, resolving underlying problems, enabling changes, tracking configurations, and setting service levels. With its fourth iteration, new ideas entered the picture: the Service Value System appeared alongside the Service Value Chain. These work in tandem, shaped by core guidelines meant to support adaptability. Focus shifts toward delivering tangible worth within tech-evolved businesses. The aim is aligning practice with real-world digital demands[3].

4.3. ITSM, IT assets, and service quality

Focused on real-world use, ITSM shapes the way technology resources, like systems, tools, apps, or information, are managed from start to finish. Studies along with field insights show stronger ITSM practices tend to go hand-in-hand with fewer outages, quicker problem fixes,

[1] - Axelos et al (2025), Op. Cit, p.29.
[2] - Bharadwaj A. et al (2013), Op. Cit, p.481.
[3] - Karydas Christos, Chatziantoniou Myrto, Stamkopoulos Kostas, Iatrou Miltiadis, Vassiliadis Vangelis, Mourelatos Spiros, (2023), Embedding a precision agriculture service into a farm management information system - ifarma/PreFer, Smart Agricultural Technology, Volume 4,2023, p.175.

smoother updates, and steadier operations. This pattern places ITSM at the center of dependable, adaptive digital environments[1].

4.4. Strategic and organizational implications

These days, writings about ITSM tend to present it less as mere back-office work - more like a lever shaping how organizations handle digital change, spark new ideas, or manage oversight. Pulling it off well means weaving it together with areas like tracking tech assets, keeping data safe, and steering projects - not just stacking systems side by side. What often is overlooked is how much hinges on people: trust across teams, shared goals, the quiet day-to-day exchanges between tech staff and those running parts of the business. Without these softer currents, even polished processes may underperform.

5. Business Continuity and Disaster Recovery

Business continuity and disaster recovery are closely related disciplines concerned with ensuring that critical organizational functions and supporting IT systems can withstand, respond to, and recover from disruptive incidents such as natural disasters, cyber-attacks, or infrastructure failures[2]. In the information systems and risk management literature, they are treated as key components of organizational resilience, integrating technical, organizational, and governance mechanisms to minimize disruption and economic loss[3].

5.1. Business continuity

A company's ability to maintain operations after disruption lies at the heart of what people call business continuity. Functioning despite setbacks isn't automatic - it usually depends on a structured approach known as a BCMS. This framework brings together several elements: evaluating threats, analyzing impacts on key functions, designing response methods, recording procedures, preparing staff, and testing readiness now and then. Such systems tend to follow standards like ISO 22301, though exact formats can differ across organizations[4].

---

[1] - Kopperapu, R. (2024), Op. Cit, p.42.
[2] - Kaplan, A. M (2010), Op. Cit, p. 67.
[3] - Karahanna, E., & Preston, D. S. (2013). The Effect of Social Capital of the Relationship between the CIO and Top Management Team on Firm Performance. Journal of Management Information Systems, p.66.
[4] - Melzer M. et al (2025), Op. Cit, p.89.

5.2. Disaster recovery

A typical way to see disaster recovery is often viewed as part of broader business continuity, just zooming in on tech stuff. When systems go down, this field handles getting them back up. Think restoring lost data or switching operations to backup locations. These actions follow specific plans shaped by earlier risk assessments. Time limits for resuming functions matter here are called RTOs. So do targets for how much data loss is acceptable, known as RPOs. Testing whether everything works post-recovery also plays a role. What counts is not just speed but accuracy in bringing things online again.

5.3. Integrated BCDR and organizational resilience

Lately, studies have pointed to blending business continuity with disaster recovery, forming what some now call BCDR to handle disruptions more cohesively across both management and tech levels[1]. Instead of treating them separately, combining these areas helps match IT fixes with broader operational workflows. This alignment tends to strengthen how organizations bounce back, especially when hit by layered or evolving crises. Recovery is not just about restoring servers; it is tied closely to keeping key processes running. When strategy and technology respond coordinated, restarts often go smoother, even under pressure.

5.4. Standards, governance, and continuous improvement

A framework like ISO 22301 sets out how organizations can shape, apply, yet refine a BCMS from the ground up - complete with disaster recovery elements woven into daily operations. Rather than treating it as static, the approach follows a loop: plan first, act next, then review what worked, followed by adjustments where needed. Resilience here is not assumed; it is tested through regular evaluations, scrutiny of risks, and follow-up steps tailored to shifting threats. Connections to broader management practices are not tacked on. They're built in from the start[2].

[1] - Sudarat Srima, Panita Wannapiroon, Prachyanun Nilsook (2015), Design of Total Quality Management Information System (TQMIS) for Model School on Best Practice, Procedia - Social and Behavioral Sciences, Volume 174, 2015, P.2165.

[2] - Sudarat S et al (2015), Op. Cit, p.2166.

CHAPTER THREE

IT Governance and Strategy

1. **IT Governance Frameworks (COBIT, ITIL, ISO 27001)**
2. **Risk Management in IT**
3. **IT Compliance and Regulations**

Introduction

In today's technology-driven environment, organizations rely on structured IT governance frameworks such as COBIT, ITIL, and ISO 27001 to ensure that technology genuinely supports business goals, manages risk, and meets regulatory expectations in the face of growing cyber threats and exploding data volumes[1]. COBIT provides an overarching framework with domains like Evaluate-Direct-Monitor (EDM) and Align-Plan-Organize (APO) that help firms steer and optimize their IT assets to serve stakeholders more effectively. ITIL complements this by focusing on the end-to-end management of IT services[2], planning, operating, and continually improving them, to enhance reliability and service quality, while ISO/IEC 27001 establishes a formal, risk-based information security management system that structures how sensitive information is protected. Recent studies emphasize that these frameworks deliver the most value when used together: COBIT offers strategic oversight, ISO 27001 supplies concrete security controls, and ITIL embeds these practices into day-to-day operations, collectively improving audit quality and reducing risk[3]. This chapter examines how combining these frameworks can strengthen IT governance, risk management, and compliance in contemporary organizations.

1. IT Governance Frameworks (COBIT, ITIL, ISO 27001)

The role of information technology has fundamentally shifted in the modern business landscape. It’s no longer just about keeping systems running in the background, technology now shapes how organizations innovate, compete, and create value.

Strategic planning around IT matters because it forces companies to think carefully about where they put their resources. When technology investments actually support business goals, rather than existing in isolation, they start to make real sense.

Before making of any major move, firms must consider how technology fits with their broader aims, this clarity shapes smarter decisions. Where digital spending lines up with company targets, value becomes visible. The link between technology and business goals goes extends beyond ideas on paper, done well, results show up clearly, workflows become smoother, people interact with companies more easily, one gains edge over competitors. Reaching that point involves not merely purchasing tools, success comes only when each part of an organization moves together with purpose.

---

[1] - Ekman P. et al (2022), Op. Cit, p.103.
[2] - Bughin, J., et al. (2018). Notes from the AI frontier. McKinsey Global Institute, p.287.
[3] - Langer A. et al., (2018), Op. Cit, p. 223.

1.1.Definition and Scope

IT strategic planning sets where technology should head, matches it with company aims. Picking what's working now, guessing what'll be needed later, building steps for spending on tools that help reach targets[1].

Strategic Alignment means how well IT matches up with business goals, operations, and setup[2]. It happens through ongoing effort - and shows results when tech leadership works right.

1.2.Theoretical Foundations

1.2.1. Strategic Alignment Model (SAM)

The strategic Alignment Model continues influencing connection beteween firm operation and environment. Built in 1993 by Henderson and Venkatram, it emphasizes fit between internal processes and external demands. Rather than treating technology as an add-on, the framework shows how digital capabilities shape strategic direction. Its lasting relevance emerges even amid newer approaches. At the core lie two overarching themes, each holding two linked components. These parts function not in isolation but as interdependent forces guiding organizational coherence.IT with business aims is built around four connected areas grouped under two main categories.

A) Domains

a) Business Strategy: Business strategy defines the long-term plan of action adopted by an organization to achieve its competitive goals. It involves the selection of markets, value propositions, customer segments, and methods of competitive advantage (e.g., cost leadership, differentiation).[3]

b) IT Strategy: IT strategy outlines how an organization's technology investments, capabilities, and initiatives will support or shape business strategy. It defines the technological direction, innovation priorities, and information systems architecture[4].

c) Organizational Infrastructure and Processes: This refers to the **structural, human, and procedural** components that enable the implementation of business strategy. It encompasses the formal organizational design, roles, reporting lines, business processes, and decision-making styles[5].

---

[1]- Luftman, J., et al (2007), Op. Cit, p.173.
[2] - Henderson, J. C., et al, p.12.
[3]- Porter, M. E. (1996). Op.Cit, p.70.
[4]- Byrd, T. A., et al (2001). Op.Cit, p.50.
[5] - Hammer, M., & Champy, J. (1993). Reengineering the Corporation: A Manifesto for Business Revolution.

d) IT Infrastructure and Processes: This includes the technical and procedural foundation for delivering IT services and supporting business operations. It comprises hardware, software, networks, databases, service management processes, and IT personnel[1].

Strategic alignment is achieved when there is coherence among these domains, both externally (strategy) and internally (infrastructure).

1.2.2. Resource-Based View (RBV):

Based on RBV, IT assets can give lasting edge when they're useful, uncommon, hard to copy, and irreplaceable. So, planning around tech should center on creating distinct abilities that fit company goals instead[2].

1.2.3. Core Assumptions of RBV

RBV is built on two main assumptions:

- Resource Heterogeneity: Organizations possess different bundles of resources.
- Resource Immobility: Certain resources cannot be easily transferred or copied across firms.

These assumptions suggest that firms with unique resources and capabilities can sustain competitive advantage over time.

1.2.4. Types of Resources

RBV classifies resources into three broad categories:

- **Tangible Resources**: Physical assets such as infrastructure, IT hardware, financial capital.
- **Intangible Resources**: Brand reputation, proprietary technology, intellectual property, organizational culture.
- **Human Resources**: Skills, expertise, leadership, and experience of employees.

Barney (1991) emphasized that not all resources contribute equally to performance. Only those with **VRIN characteristics(*)** lead to sustained competitive advantage.

(*) VRIN = Valuable, **R**are, **I**nimitable, **N**on-substitutable.

[1] - Weill, P., & Broadbent, M. (1998). *Leveraging the New Infrastructure: How Market Leaders Capitalize on Information Technology.* Harvard Business School Press, p.85.

[2] - Wade & Hulland, 2004.

1.3. Importance and Benefits

Achieving balance between tech systems and company aims matters a lot these days. If tech plans match actual business targets, companies gain clear advantages plus, less obvious ones, that boost how they perform and where they stand against rivals[1].

1.4. Enhanced Decision-Making Through Data and Analytics

Aligning IT with business proves valuable when smarter decisions emerge from reliable data systems that quickly reveal patterns. Research by Kappelman shows that firms coordinating these areas tend to develop integrated data networks, which enable managers to receive real-time insights while issues are still small. In an environment of constant information flow, responding swiftly and clearly becomes less about gaining an advantage and more about simply staying relevant.

1.5. Improved Organizational Agility

IT governance frameworks help improve organizational agility by providing structured decision rights, processes, and accountability that enable faster, better-aligned IT enabled change. They clarify who can prioritize and approve IT investments, which reduces obstacles and accelerates response to new business requirements. By enforcing standards, architectures, and risk controls, they create a stable yet flexible

1.6. Optimized Resource Allocation and Value Realization

When IT matches company goals, money goes to what matters most cutting down on pointless projects. That shift strengthens oversight, so tools, people, and funds are not spread thin without purpose. Instead of random picks, choices follow real needs, boosting results from tech spending. Matching digital plans with core aims helps teams get more out of every dollar put into systems.

1.7. Greater Stakeholder Engagement and IT Credibility

When IT leaders work closely with business managers, misunderstandings drop off. Because of this teamwork, people across the company start trusting tech teams more. Instead of seeing IT as just an expense, they begin viewing it as a key player. With better sync, tech

[1] - Kappelman, L., McLean, E., Johnson, V., & Torres, R. (2019). The 2019 SIM IT Issues and Trends Study. MIS Quarterly Executive, 18(1), 1–20.

units get invited into major planning talks. Being part of big decisions weaves IT deeper into how companies move forward.

1.8. Empirical Performance Outcomes

A good chunk of real-world studies shows how well tech goals matching business aims can boost company results[1]. Research keeps revealing that companies where these two sides sync up:

- Achieve **higher financial performance** (e.g., ROI, profit margins).
- Improve **operational efficiency**, through reduced redundancy and better process integration.
- Enhance **customer satisfaction**, by leveraging IT to deliver superior user experiences.

Research finds companies matching IT with business goals do better financially, work more smoothly, yet keep customers happier [2].

1.9. Key Components of IT Strategic Planning

IT strategic planning is a structured process that ensures information technology (IT) investments, initiatives, and capabilities align with and support an organization's strategic objectives. This process comprises several interrelated components, each playing a crucial role in shaping IT's contribution to long-term business success.

1.9.1. IT Vision and Mission

A solid IT vision shows where tech should go in the long run, whereas the mission explains what it does daily. One points ahead, the other grounds current work in company beliefs. These ideas link teams around one goal without confusion piling up. They also make it easier to spread the message clearly through different departments.

1.9.2. Environmental Scanning

Looking at what's happening inside and outside a company can shape how it uses tech. Keeping an eye on new tools - say, artificial intelligence or online storage - matters quite a bit. So does watching what rivals are up to or big shifts shaking up industries. Rules around data

[1] - Chan, Y. E., Sabherwal, R., & Thatcher, S. M. B. (2006). Antecedents and outcomes of strategic IS alignment: An empirical investigation. *IEEE Transactions on Engineering Management*, 53(1), p.27.
[2] - Chan et al., (2006), Op. Cit, p. 34.

use, such as GDPR, also play a role. Knowing all this lets businesses prepare ahead of time instead of reacting late. They can then spend wisely on technology while staying ready for surprises.

1.9.3. SWOT Analysis for IT

A SWOT check - looking at strengths, weaknesses, chances, or dangers - gives a clear picture of what the IT team can do well or where it struggles, along with outside factors that could help or hurt. It highlights spots needing upgrades, like old software, while pointing out strong skills such as data crunching ability. New customer bases might open up, yet things like hacking worries stay real risks[1]. These insights shape big-picture goals just as much as they guide ways to dodge problems.

1.9.4. IT Roadmap

The IT roadmap's basically a broad outline showing particular actions, schedules, checkpoints, also tracked results - all tied to company aims. Instead of just listing plans, it turns big-picture targets into real tasks plus spending choices, shaping day-to-day work along with future shifts. A solid version keeps tech efforts running smoothly - hitting deadlines, staying on budget, while delivering clear impact[2].

1.9.5. Governance Structures

Governance sets clear rules so tech choices match company goals while sticking to laws and ethics. Instead of just meetings, groups like oversight teams or planning panels help guide IT direction. Such setups improve coordination, keep actions visible, while helping leaders pick better paths between departments[3].

1.9.6. Performance Management

Performance management involves tracking and evaluating the effectiveness of IT initiatives through metrics, dashboards, and feedback loops. Common KPIs include ROI on IT investments, system uptime, project delivery success rates, and user satisfaction. This

[1] - Kappelman, L., McLean, E., Johnson, V., & Torres, R. (2019). The 2019 SIM IT Issues and Trends Study. MIS Quarterly Executive, 18(1), 1–20.

[2] - Ayat, M., & Shafiee, S. (2025). Integrating COBIT 2019 and ISO/IEC 27001 for Strengthening IT Governance and Information Security. Proceeding of the International Conference on Economics, Business, Science, and Technology, p73.

[3] - Weill, P. et al, (1998), Op. Cit, p. 187.

component supports continuous improvement and reinforces strategic alignment by demonstrating IT's contribution to business value[1].

Performance management means keeping an eye on how well tech projects are doing using numbers, visual reports, or regular check-ins. Typical measures, return from tech spending, time systems stay running, whether projects finish on target, also how happy users feel. It helps things get better over time while making sure tech work lines up with company goals, showing real impact on results.

1.10. Challenges in Achieving Strategic Alignment through IT Governance Frameworks

The alignment of Information Technology (IT) strategy with business goals, often termed Business-IT Alignment (BITA), remains a persistent challenge for modern enterprises. While governance frameworks such as COBIT (Control Objectives for Information and Related Technologies), ITIL (Information Technology Infrastructure Library), and ISO/IEC 27001 provide structural guidance, their practical implementation is frequently obstructed by complex organizational, cultural, and structural barriers[2].

The following analysis explores these challenges, drawing upon recent academic literature to highlight the friction points in utilizing these frameworks for strategic planning.

1.10.1. The "Siloization" and Cultural Divergence

One of the most cited barriers to alignment is the cultural and linguistic divide between IT and business units. Frameworks like ITIL focus heavily on service delivery metrics (e.g., uptime, incident resolution), which often fail to translate into the value-based language spoken by executive boards[3].

---

[1] - Weill, P. et al, (1998), Op. Cit, p. 205.
[2] - Ayat, M., & Shafiee, S. (2025). Integrating COBIT 2019 and ISO/IEC 27001 for Strengthening IT Governance and Information Security. Proceeding of the International Conference on Economics, Business, Science, and Technology, p73.
[3] - Henderson, J. C., et al, Op. Cit, p.13.

- **Communication Gaps:** A significant inhibitor is the lack of a shared domain knowledge. Business executives often view IT governance as a technical compliance exercise rather than a strategic enabler. Conversely, IT managers may struggle to articulate how technical controls (e.g., ISO 27001 security protocols) directly support market expansion or revenue growth[1].

- **Cultural Resistance:** Implementing frameworks like COBIT requires a shift from a "support function" mindset to a "strategic partner" mindset. Research indicates that without a corresponding shift in organizational culture, governance mechanisms become rigid bureaucracies that stifle innovation rather than aligning it with business needs[2].

Figure 3.1: Strategic Alignment

Source: synthesized by the author based on McKenney (1995), Laudon (2021).

1.10.2. Framework Complexity and Integration Fatigue

Organizations rarely use a single framework in isolation. The simultaneous adoption of COBIT (for high-level governance), ITIL (for service management), and ISO 27001 (for security) creates an "integration paradox" where the complexity of managing the frameworks themselves overshadows their strategic intent.

[1] - Karahanna, E., et al (2013). Op. Cit, p175.
[2] - Melaku, B. (2023). Barriers to Effective IT Governance in Developing Economies. African Journal of Information Systems, p.92.

- **Lack of Native Interoperability:** While COBIT is designed to be an umbrella framework, mapping its objectives to the specific controls of ISO 27001 or the service lifecycles of ITIL is manually intensive. A 2025 study noted that the absence of automated integration between governance (COBIT) and security (ISO 27001) leads to "fragmented accountability" and overlapping controls that confuse strategic direction[1].

- **The "Checklist" Trap:** There is a tendency to treat ISO 27001 and ITIL as operational checklists rather than strategic tools. When organizations focus solely on achieving certification (e.g., passing an ISO audit), they often decouple these activities from the broader business strategy, leading to a phenomenon known as "strategic drift"[2].

- **Resource Constraints and Lack of Executive Sponsorship**

Academic literature consistently identifies the lack of sustained executive sponsorship as a primary failure mode for IT governance[1].

- **Perceived Bureaucracy vs. Agility**

In fast-paced markets, the rigorous documentation and process controls required by ISO 27001 and COBIT are often perceived as impediments to agility. SMEs, in particular, face "resource poverty," where the cost and time required to align IT strategic planning with formal frameworks are viewed as disproportionate to the immediate business value[3].

- **Inadequate Skills:** Effective alignment requires "hybrid" managers who possess both technical acumen and strategic business insight. The scarcity of such talent means that technical specialists who lack the authority or perspective to enforce alignment at the board level often implement governance frameworks[4].

[1] - Rizal et al., 2025, Op. Cit, p.119.
[2]- Tsiu, T., et al. (2024). The Impact of IT Strategic Planning Process on SME Performance: A Systematic Review. MDPI, Journal of Open Innovation, p.117.
[3] - Rizal et al., 2025, Op. Cit, p.120.
[4] - Ayat, M., & Shafiee, S. (2025), Op. Cit, p.223.

Table 2.1: Key Takeaways for Practitioners

Challenge Domain	Primary Issue	Impact on Strategic Alignment
Cultural	Language gap between IT & Business	IT KPIs (e.g., uptime) do not map to Business KPIs (e.g., ROI).
Structural	Integration complexity	Overlapping controls between COBIT/ISO lead to audit fatigue rather than strategy.
Operational	"Checklist" mentality	Governance becomes a compliance burden rather than a strategic enabler.

Source : (Ayat & Shafiee, 2025).

2. Risk Management in IT

Risk Management in IT (often termed IT risk management or ITRM) denotes the systematic application of risk management methods to information technology in order to identify, assess, treat, and monitor risks that could compromise the confidentiality, integrity, or availability of information and IT services. In the academic and professional literature, IT risk management is framed as a core component of enterprise risk management and information security management, linking technical vulnerabilities and threats to business-level impacts and decision making[1].

Figure 3.2: Risk Context and Scope in Risk Management Processes

Source: Laudon (2021)

[1] - Taherdoost Hamed, Madanchian Mitra (2022), Employment of Technological-Based Approaches for Creative E-Learning; Teaching Management Information Systems, Procedia Computer Science, Volume 215, 2022, P. 805.

2.1. Conceptual Frameworks and Standards

Conceptually, IT risk management seeks to control the likelihood and impact of adverse events arising from IT-related threats such as cyber-attacks, system failures, misconfigurations, or human error, within levels acceptable to the organization's risk appetite. Typical objectives include safeguarding information assets, ensuring regulatory and contractual compliance, supporting service continuity, and aligning IT-related risk with overall enterprise risk strategies.[1]

2.1.1. Processes and lifecycle

IT risk management processes generally follow an iterative lifecycle comprising context establishment, risk identification, risk analysis and evaluation, risk treatment, and ongoing monitoring and review. Within this lifecycle, organizations identify assets, threats, and vulnerabilities; estimate likelihood and impact; prioritize risks; and select treatment options such as mitigation through controls, risk transfer, risk avoidance, or formal risk acceptance.

2.1.2. Frameworks and standards

Several frameworks guide IT risk management practice, including ISO/IEC 27005 for information security risk management, NIST SP 800-37 for risk management in federal information systems, and COBIT, which integrates IT governance and risk optimization principles[2]. At the enterprise level, COSO ERM provides a broader risk management umbrella, while COBIT offers a more IT-focused structure that aligns IT objectives, controls, and risks with business goals.

2.1.3. Relationship to information security and governance

In many organizations, IT risk management is embedded within an Information Security Management System (ISMS) certified against ISO/IEC 27001, where risk assessment and treatment provide the basis for selecting and justifying security controls (ISO 27005 guidance; DataGuard, 2024). As such, IT risk management is closely linked to governance, compliance, and audit functions, providing structured evidence of how IT-related risks are identified, evaluated, and controlled in line with legal, regulatory, and stakeholder expectations.

[1] - Abdullah, Ojo & Martin, Saheed. (2022). Risk Management Frameworks in Cybersecurity and Digital Investigations.

[2] - Swapan Basu (2024), Chapter 14 - Management information system (MIS), Editor(s): Swapan Basu, Plant Intelligent Automation and Digital Transformation, Academic Press, 2024, P.402.

2.1.4. ISO 31000: The Enterprise Risk Management Standard

ISO 31000 provides the principles and general guidelines for risk management across the entire organization, forming the foundation for most IT-specific standards. Its process involves[1]:

- ❖ **Establishing the Context**: Defining the scope, criteria, and objectives of the risk management activity in alignment with the organization's strategic goals[2].
- ❖ **Risk Assessment**: Encompassing Risk Identification (recognizing sources of risk), Risk Analysis (determining likelihood and impact), and Risk Evaluation (comparing assessed risk levels with risk criteria).
- ❖ **Risk Treatment**: Selecting and implementing options for modifying risks, which can include avoidance, reduction (mitigation controls), sharing (transfer), or retention.

2.2. Key Challenges in Effective IT Risk Management

Despite the availability of robust frameworks, organizations frequently face challenges that prevent the establishment of a mature and effective IT risk management program:

2.2.1. Subjectivity in Risk Assessment: A significant challenge is the lack of objectivity in assigning asset values and assessing the probability and impact of threats[3]. This subjectivity often leads to resource allocation that prioritizes high-profile but less likely risks, while overlooking critical, high-probability risks. Methodologies like FAIR (Factor Analysis of Information Risk) are gaining academic recognition for attempting to quantify risk in financial terms to mitigate this bias[4].

2.2.2. The Compliance-Centric Trap: Many organizations treat IT risk management primarily as a compliance exercise to meet regulatory requirements, rather than an integrated mechanism for strategic decision-making[5]. This focus on checking boxes rather than managing actual threat exposure leads to a risk program that is documented but not operationally effective.

2.2.3. Lack of Top Management Commitment and Integration: Effective risk governance requires executive leadership to set the risk appetite and allocate sufficient

---

[1] - Efe, Doç. Dr. Ahmet. (2023). A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT, p.22.
[2] - Efe, Doç. Dr. Ahmet. (2023), op. Cit, p27
[3] - Metin, B., et al. (2024). IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture. Information, 15(1), p.55.
[4] - Tsiu, T., et al**.** (2024).Op. Cit, p.124.
[5] - Efe, A. et al (2023), Op. Cit., p.32.

resources[1]. When risk management operates in an IT silo, disconnected from business strategy and capital planning, it fails to provide the holistic, 360-degree view of risk required in modern, interconnected digital environments[2].

2.2.4. Dynamic and Distributed Risk Landscape: The rise of technologies like Cloud Computing, IoT, and complex supply chain dependencies has made the risk landscape highly dynamic and distributed [3]. Traditional, annual risk assessment methods often fail to keep pace, necessitating the adoption of continuous monitoring and the leverage of advanced techniques like Artificial Intelligence (AI) for real-time threat detection[4].

3. IT Compliance and Régulations

Information Technology (IT) compliance is the practice of ensuring that an organization's use of IT systems, assets, and processes adheres to mandatory external laws, regulations, and industry standards, as well as voluntary internal policies[5]. In an increasingly data-driven global economy, regulatory adherence is inextricably linked to IT governance and risk management, moving from a purely defensive activity to a core strategic imperative.

3.1. Major Global Regulatory Frameworks

The global landscape of IT regulation is characterized by a fragmented and evolving set of laws and standards, primarily focused on data privacy, security, and financial integrity.

[1] - Efe, A. et al (2023), Op. Cit., p.33.
[2] - Metin, B., et al. (2024).
[3] - Melaku, B. (2023). *Barriers to Effective IT Governance in Developing Economies*. *African Journal of Information Systems*.
[4] - Rizal et al., 2025, Op. Cit, p.122.
[5] - ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association.

Table 2.2: Major Global Regulatory and Compliance Frameworks Governing IT and Data Assets

Regulation/Standard	Jurisdiction/Applicability	Core Focus	Protected Data
GDPR (General Data Protection Regulation)	European Union (EU) and any organization processing EU resident data	**Data Privacy and Individual Rights**	Personal Data (PI)
HIPAA (Health Insurance Portability and Accountability Act)	United States (U.S.) Healthcare Sector	**Health Data Confidentiality and Security**	Protected Health Information (PHI)
PCI DSS (Payment Card Industry Data Security Standard)	Global (All entities that process, store, or transmit cardholder data)	**Payment Card Security and Fraud Prevention**	Cardholder Data
SOX (Sarbanes-Oxley Act)	U.S. Publicly Traded Companies	**Financial Reporting Integrity and Controls**	Financial and Accounting Data
ISO/IEC 27001	Global (Voluntary International Standard)	**Information Security Management System (ISMS)**	All Information Assets

Source: Efe, A. (2023). A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. Journal of Auditing and Assurance Services, 3(2).

3.1.1. Data Privacy Legislation (GDPR, HIPAA, CCPA)

These regulations legally mandate specific technical and organizational controls to protect personal information, empowering individuals with rights such as the right to access, erasure and data portability[1].

- **GDPR's Extraterritorial Reach:** GDPR is notable for its strict fines and its requirement for Privacy-by-Design, mandating that privacy considerations be incorporated into systems and processes from the initial design phase[2].
- **HIPAA's Security Rule:** HIPAA requires specific safeguards, administrative, physical, and technical, to secure electronic Protected Health Information (ePHI), forcing healthcare organizations to implement encryption, access controls, and audit logs[3].

3.1.2. Industry-Specific and Financial Standards (PCI DSS, SOX)

These standards dictate security requirements for critical business processes, primarily financial ones.

- **PCI DSS:** While not a government regulation, compliance with this standard is mandatory for any organization handling payment card data and is enforced by card

[1] - Kopperapu, R. (2024), Op. Cit, p.43.
[2] - Kopperapu, R. (2024), Op. Cit, p.44.
[3] - Wang, T., et al. (2024). Op. Cit, p.26.

brands. It requires 12 core security requirements, including network segmentation and encryption of data in transit and at rest[1].

- **SOX:** This law focuses on the integrity of financial reporting. IT compliance under SOX centers on the IT General Controls (ITGCs), specifically access management, change management, and operations controls, that ensure the reliability of the financial data residing in corporate systems[2].

3.2. Challenges in Achieving IT Regulatory Compliance

Navigating the contemporary compliance landscape poses significant organizational, operational, and financial challenges, particularly for multinational corporations:

3.2.1. Regulatory Fragmentation and Overlap

Organizations operating across multiple countries face a "patchwork" of conflicting or overlapping regulatory requirements[3].

- **Jurisdictional Conflicts:** Companies must reconcile standards like GDPR (EU) with CCPA (California) or PIPL (China), which may have different definitions of "personal data" or conflicting rules regarding cross-border data transfer[4]. This regulatory ambiguity complicates compliance efforts and requires specialized legal and technical expertise[5].
- **Harmonization Complexity:** While frameworks like ISO 27001 and NIST CSF (Cybersecurity Framework) are often used to provide a unified technical baseline, mapping the controls of a single Information Security Management System (ISMS) to the varying legal requirements of multiple regulations remains a costly and continuous manual exercise[6].

3.2.2. Dynamic Technological Change

The compliance landscape is in a constant state of flux, often lagging behind the rapid pace of technological innovation.

- **Emerging Technologies:** New technologies, such as Generative AI and advanced cloud architectures, introduce novel risk vectors and compliance gaps that existing regulations

[1] - Rizal et al., 2025, Op. Cit, p.124.
[2] - Efe, A. (2023), Op. Cit, p.35
[3] - Blind, K., et al. (2023). Regulatory Fragmentation in the Digital Economy. Journal of Policy Research, p.55.
[4] - Wang, T., et al. (2024), Op. Cit, p. 27.
[5] - Blind, K., et al. (2023), Op. Cit, p. 62.
[6] - Rizal, A., et al. (2025), Op. Cit, p.125.

struggle to address[1]. This forces regulators to continuously issue new guidance, which organizations must rapidly absorb and implement.

- **Continuous Monitoring Requirement:** Compliance is not a static state achieved by passing an annual audit but an ongoing process. The increasing frequency of updates and the need to monitor system configurations and data access in real-time necessitate the adoption of RegTech (Regulatory Technology) tools to automate evidence collection and continuous control enforcement[2].

3.2.3. Resource and Cultural Constraints

Achieving compliance requires substantial investment and a fundamental cultural shift within the organization.

- **High Compliance Cost:** The financial and operational cost of compliance, including personnel, training, and security technology, is substantial. For SMEs (Small and Medium-sized Enterprises), this cost can be disproportionate to their revenue, often creating a barrier to entry into regulated markets[3].
- **Compliance vs. Security Mindset:** Organizations often adopt a "check-box" compliance mentality, implementing the bare minimum controls required to pass an audit without integrating those controls into a proactive, threat-aware security posture. This approach leads to fragile security and increased vulnerability despite technical "compliance"[4].

[1] - Protiviti. (2025). Top compliance challenges facing the technology industry in 2025. Protiviti Global, p.102.
[2] - Rippling. (2025). What Is IT Compliance? Risks, Best Practices, & Checklist (2025). Rippling Blog. p.56.
[3] - Tsiu, T., et al. (2024), Op. Cit, p. 125
[4] - Efe, A. (2023), Op. Cit, p.36.

CHAPTER FOUR

Innovation and Digital Transformation

1. **IT, Organizations, and Strategic Alignment**
2. **Strategic Alignment Model (SAM)**
3. **Information systems strategy and organizational structure**
4. **IT capabilities and competitive advantage**
5. **Innovation and Digital Transformation**

Information Technology (IT) management, organizational design, and business strategy are deeply interdependent domains, with research consistently showing that the way IT is governed and deployed can enable or constrain strategic options and organizational performance[1]. Modern organizations therefore treat IT not merely as an operational support function but as a strategic resource that must be aligned with business goals, structures, and processes to generate competitive advantage.

1. IT, Organizations and Strategic Alignment

IT, organizations, and strategic alignment are linked through the idea that information technology must be purposefully configured and governed to support and shape business strategy, organizational structures, and processes rather than operating as an isolated technical function[2]. The alignment literature treats IT as both a strategic resource and an organizational capability whose value depends on fit with the firm's competitive positioning, decision structures, and patterns of collaboration across business units.

1.1. Concept of business–IT strategic alignment

Business-IT strategic alignment is commonly defined as the degree of coherence and mutual reinforcement between business strategy, IT strategy, organizational infrastructure, and IT infrastructure[3]. Empirical studies and reviews show that higher alignment is associated with improved performance, innovation, and agility, but also stress that alignment is dynamic and must be continuously managed in response to environmental and technological change.

1.2. Strategic Alignment Model (SAM)

The Strategic Alignment Model (SAM) distinguishes between external domains (business strategy and IT strategy) and internal domains (organizational infrastructure/processes and IT infrastructure/processes), arguing that strategic fit (external–internal) and functional integration (business–IT) are both required for effective use of IT. Subsequent research uses SAM to analyze alignment "paths" (for example, strategy execution, technology transformation, competitive potential, and service level) that describe how changes in business strategy or IT capabilities propagate through organizational structures and systems.

[1] - Henderson et al (1993), Op. Cit, p. 14.
[2] - Tsiu, T., et al. (2024), Op. Cit, p. 127.
[3] - McAfee, A. et al (2012), Op. Cit, p. 64.

1.3. Organizational structure, governance, and IT

Alignment research emphasizes that organizational arrangements—such as centralization of IT, distribution of decision rights, and the design of IT governance mechanisms—mediate the relationship between IT and strategy[1]. Misfits between information systems strategy and organizational structure are associated with coordination problems, underutilized systems, and difficulties in realizing expected strategic benefits.

1.4. IT capabilities as strategic assets

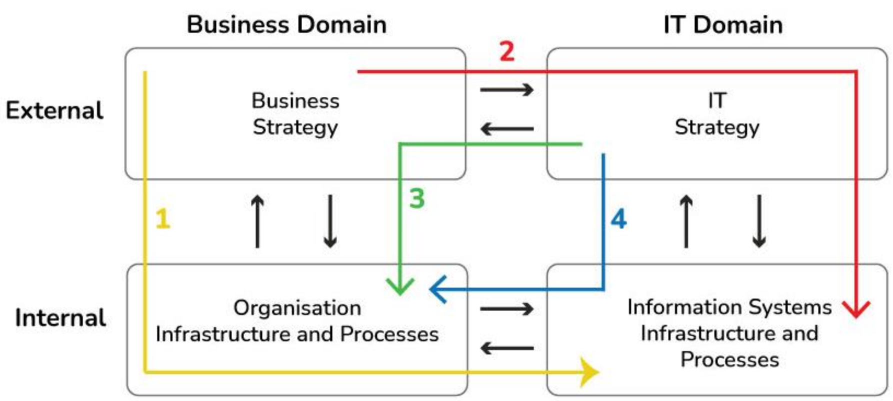
Drawing on the resource-based view, several studies argue that IT resources contribute to competitive advantage when they are combined with organizational capabilities such as process redesign, cross-functional integration, and data-driven decision-making routines[2]. In this perspective, strategic alignment involves configuring IT infrastructure, applications, and human skills so that they enable and reinforce the firm's chosen strategic posture across organizational units.

2. Strategic Alignment Model (SAM)

The Strategic Alignment Model (SAM) is a conceptual framework developed by Henderson and Venkatraman to explain how organizations can systematically align business strategy and information technology (IT) strategy to create value and sustain competitive advantage. It argues that the benefits of IT investments depend less on individual applications and more on the coherent alignment of strategies and infrastructures across business and IT domains within the organization.

[1] - Floridi, L. et al (2019), Op. Cit., p.169.
[2] - McAfee, A. et al (2012), Op. Cit, p. 65.

Figure 4.1: Strategic Alignment Model (SAM)



Source: synthesized by the author based on Applegate et al. (2003) and Ceruzzi (2003).

2.1. Core structure of SAM

The core structure of the Strategic Alignment Model (SAM) consists of four interrelated domains organized along two conceptual dimensions, external vs. internal focus and business vs. IT focus[1].

2.1.1. Four domains

- **Business strategy (external, business)**: Describes how the firm competes in its markets, including business scope, distinctive competencies, and business governance.
- **IT (or IS) strategy (external, IT):** Articulates the firm’s technology vision and role of IT in the competitive arena, including IT scope, systemic competencies, and IT governance.
- **Organizational infrastructure and processes (internal, business)**: Covers administrative structure, business processes, and skills that operationalize business strategy.
- **IT infrastructure and processes (internal, IT)**: Encompasses hardware, software, data, technical architectures, and IT processes (development, operations, support) that implement IT strategy.

[1] - Xiaoming Zhang, Shina Qiao, Rongrong Zhang, Minjun Liu, Lili Wu, Hongying Pan (2023), Construction and Application of Chain Management Information System for Cancer Pain, Pain Management Nursing, Volume 24, Issue 4, 2023, P.79.

2.2. Alignment perspectives in SAM

In the Strategic Alignment Model (SAM), alignment perspectives describe alternative "lenses" through which business–IT alignment can be conceived and managed, each emphasizing different cross-domain relationships between business and IT strategy and infrastructures. These perspectives are central to understanding how organizations can configure responsibilities and governance to leverage information systems for strategic advantage[1].

2.2.1. Strategy Execution perspective

The strategy execution perspective treats business strategy as the primary driver, cascading into organizational structure and, in turn, into IT infrastructure and processes. In this view, top management formulates business strategy, business managers design organizational infrastructure, and IT management implements the required systems to support predetermined strategic goals, reinforcing a classic, hierarchical conception of strategic management[2].

2.2.2. Technology Potential perspective

The technology potential perspective also starts from business strategy, but explicitly introduces IT strategy as an intermediate layer that translates business intent into a coherent technology vision. Here, senior executives articulate a technology strategy aligned with business priorities, while IT leadership assumes the role of "technology architect," designing IT infrastructure and processes that realize this vision and ensure that technological capabilities are exploited systematically[3].

2.2.3. Competitive Potential perspective

The competitive potential perspective emphasizes how emerging IT capabilities can reshape business strategy itself, rather than merely supporting an existing strategic posture. IT is conceptualized as a source of innovation that can redefine business scope, distinctive competencies, and governance arrangements, enabling new products, services, or industry structures and requiring close, interactive collaboration between business and IT leaders[4].

1- Shi, W., et al. (2016), Op. Cit, p.646.
2- Senna P, da Cunha Reis A, Castro A, Dias AC (2020), Promising research fields in supply chain risk management and supply chain resilience and the gaps concerning human factors: A literature review. Work. 2020;67(2): p.498.
3 - Peppard, J., & Ward, J. (2004), Op. Cit, p.191.
4 - Nambisan, S (2017), Op. Cit, p.229.

2.2.4. Service Level perspective

The service level perspective focuses on building a high-performing IT organization capable of delivering reliable, value-adding services to the business. In this configuration, IT strategy and IT infrastructure/processes are central, and the main concern is how IT can provide responsive, high-quality services, internal customer orientation, and operational excellence that indirectly support business strategic objectives.

2.2.5. Intellectual and social dimensions of alignment

Subsequent literature has complemented these alignment perspectives by distinguishing between intellectual (content-related) and social (relationship-related) dimensions of alignment. The intellectual dimension concerns the formal consistency between business and IT plans, architectures, and governance structures, while the social dimension captures shared understanding, mutual commitment, and collaborative practices between business and IT executives, both of which condition how effectively the four SAM perspectives can be realized in practice.

2.3. SAM in contemporary research and practice

SAM in contemporary research and practice is primarily treated as a foundational but evolving lens for understanding how organizations align IT with business strategy, especially under conditions of digital transformation and environmental dynamism[1]. Recent work tends to extend, operationalize, or critique the Strategic Alignment Model rather than replace it, emphasizing dynamic, capability-based, and ecosystem-oriented views of alignment.

2.3.1. SAM in contemporary research

Contemporary studies use SAM as a reference framework for empirical investigations of business. IT alignment, often integrating it with resource-based, dynamic-capabilities, or governance perspectives[2]. Research focuses on measuring alignment, understanding its antecedents (for example, governance mechanisms, shared understanding), and examining its impact on innovation, agility, and performance in sectors undergoing digitalization.

2.3.2. Extensions and critiques of SAM

Several authors argue that SAM is essentially static and needs extension to capture continuous, iterative alignment in turbulent environments[3]. Recent conceptual work therefore

---

[1] - Porter, M. E. (1996), Op. Cit, p.72
[2] - Porter, M. E. (1996), Op. Cit, p.75.
[3] - Venkatraman, N. (1994). IT-enabled business transformation: From automation to business scope redefinition. *Sloan Management Review, 35*(2), p73.

introduces notions such as "dynamic alignment," "digital business strategy," and "co-evolution" between IT and organization, while still using SAM's four-domain structure as a starting point.

2.3.3. SAM in practice and managerial use

In practice-oriented literature and consulting guidance, SAM is used to structure alignment assessments, maturity models, and governance designs, helping executives map relationships between business strategy, IT strategy, organizational structure, and IT architecture. Case-based reports show SAM being applied to guide IT portfolio rationalization, operating-model redesign, and the integration of new digital capabilities into existing organizations.

2.3.4. Typical figures and visual representations

Contemporary publications continue to depict SAM as a two-by-two matrix with four domains business strategy, IT strategy, organizational infrastructure/processes, and IT infrastructure/processes organized along external, internal and business, IT axes[1]. Many papers add overlays or additional figures, such as arrows indicating alignment "paths" (strategy execution, technology transformation, competitive potential, service level) or dynamic loops illustrating ongoing, iterative alignment in digital contexts

2.3.5. Enhancing Organizational Efficiency through the Strategic Alignment Model

SAM can improve organizational efficiency by forcing explicit, structured alignment between what the business is trying to achieve and how IT structures, processes, and investments are configured to support those goals. When the four SAM domains are made coherent, organizations reduce wasteful IT spending, eliminate redundant processes, and streamline decision-making across business and IT functions.

2.3.6. Clarifying roles, priorities, and decisions

By distinguishing business strategy, IT strategy, organizational infrastructure, and IT infrastructure, SAM clarifies who decides what and how those decisions must be coordinated. This reduces conflicting initiatives (for example, business units demanding bespoke solutions while IT standardizes platforms) and leads to more efficient portfolio and architecture decisions.

2.3.7. Reducing process and system misfits

SAM's focus on "strategic fit" and "functional integration" draws attention to mismatches between processes, structures, and systems (for instance, decentralized business with

[1] - Venkatraman, N. (1994). Op. Cit, p.75.

centralized IT, or cost-leadership strategy on highly customized, expensive platforms)[1]. Identifying and correcting these misfits improves process flow, reduces rework and manual workaround, and enhances the utilization of shared IT services.

2.3.8. Guiding targeted alignment paths

The four alignment perspectives (strategy execution, technology transformation, competitive potential, service level) give managers concrete “paths” for change, so that IT initiatives are sequenced and scoped according to strategic priorities. This helps avoid fragmented, project-by-project changes and instead channels resources into integrated programs that simultaneously redesign processes, structures, and systems for higher efficiency.

2.3.9. Supporting continuous coordination in dynamic environments

Because SAM emphasizes alignment as an ongoing managerial task, it supports continuous review of how IT capabilities and organizational arrangements adapt to new strategies and environmental shifts. Organizations that institutionalize this review (for example, via joint business, IT governance forums) tend to detect misalignment earlier, adjust architectures more systematically, and maintain higher operational efficiency over time.

2.3.10. Challenges in Implementing the Strategic Alignment Model

Implementing the Strategic Alignment Model (SAM) is challenging because it requires simultaneous change in strategy, structures, processes, and IT, rather than isolated IT projects. Organizations often struggle to operationalize the abstract concepts of “strategic fit” and “functional integration” in day-to-day governance and decision-making[2].

2.3.11. Conceptual and measurement difficulties

SAM is a high-level conceptual model, so translating its four domains and alignment perspectives into concrete metrics, roles, and processes is non-trivial. Empirical work shows that many firms lack reliable instruments to assess the degree of business–IT alignment, making it hard to monitor progress or justify alignment initiatives[3].

2.3.12. Organizational and cultural barriers

Implementing SAM often exposes structural conflicts, such as centralized IT versus decentralized business units, or different time horizons between business and IT planning

[1] - Venkatraman, N. (1994). Op. Cit, p.82.
[2] - Reich, B. H., & Benbasat, I. (2000). Factors that influence the social dimension of alignment between business and information technology objectives. MIS Quarterly, 24(1), p.110.
[3] - Rizal, A., et al. (2025), Op. Cit, p.125.

cycles. Resistance to change, siloed cultures, and weak collaboration between business and IT stakeholders hinder the cross-functional integration that SAM presupposes[1].

2.3.13. Dynamic environments and sustaining alignment

Alignment is not a one-off state but a moving target, especially under digital transformation, new business models, and rapidly evolving technologies. Studies report that even when alignment is achieved at a point in time, organizations find it difficult to sustain as strategies, markets, and technologies co-evolve.

2.3.14. Governance and capability constraints

Effective use of SAM requires mature IT governance, portfolio management, and architectural capabilities, which many organizations lack or only partially possess. Without clear decision rights, joint planning mechanisms, and sufficient strategic IT skills, SAM risks remaining a theoretical reference rather than a practical guide for investment and design decisions[2].

3. Information systems strategy and organizational structure

Information systems (IS) strategy and organizational structure are tightly interwoven, because choices about applications, data, and IT infrastructure both shape and are shaped by how activities, decision rights, and coordination mechanisms are organized in the firm[3]. Research shows that misalignment between IS strategy and organizational structure often leads to underutilized systems, coordination failures, and limited strategic impact of IT.

3.1. Definitions and Conceptual Foundations

Conceptual foundations refer to the underlying ideas, theories, and principles that explain why a phenomenon is understood and analyzed in a particular way. They function as a conceptual "ground" for the study, showing how existing knowledge, models, and assumptions inform the design of research questions, methods, and interpretations.

3.2. Information Systems Strategy

In the information systems (IS) literature, information systems strategy is generally understood as the pattern of decisions that governs how an organization invests in, deploys,

[1] - Shapiro, C et al (1999), Op. Cit, p.159.
[2] - Shapiro, C et al (1999), Op. Cit, p.160.
[3] - Lederer, A. L., & Sethi, V. (1996). Toward a theory of strategic information systems planning. Journal of Strategic Information Systems, 5(3), p.247.

uses, and manages IS to support and shape its business objectives[1]. It is distinct from, but tightly coupled to, business strategy, because it defines the role of IS in creating value, enabling processes, and sustaining competitive advantage.

3.2.1. Definition and core concept

Recent reconceptualization work defines IS strategy as an "organizational perspective on the investment in, deployment, use, and management of IS," emphasizing that it is not just a plan but an ongoing viewpoint shared by key stakeholders. Earlier definitions describe IS strategy as bringing together business aims, information needs, and the implementation of computer systems into a coherent plan for the future role of IS in the organization[2].

3.2.2. Main conceptions in the literature

A major review by Chen et al. identifies three dominant conceptions of IS strategy in academic work: IS strategy as the use of IS to support business strategy, as the master plan of the IS function, and as a shared view of the role of IS in the organization[3]. These views collectively underline that IS strategy concerns both what IS should do for the business (support, transform, innovate) and how the IS function is organized to deliver that contribution.

3.2.3. Relationship to strategic information systems planning

Strategic information systems planning (SISP) is treated as the process dimension through which IS strategy is formulated and implemented, involving stages such as strategic awareness, situation analysis, strategy conception, formulation, and implementation. Effective SISP aligns portfolios of applications and infrastructure with corporate strategy, ensuring that IS strategy is grounded in analyses of data needs, environmental conditions, and organizational capabilities[4].

3.2.4. IS strategy in the digital age

More recent work on IS/IT strategy in the digital era highlights shifts toward digital platforms, ecosystems, and agility, arguing that IS strategy is increasingly inseparable from digital business strategy. Reviews show that research has moved from viewing IS strategy

[1]- Chen, D. Q., Mocker, M., Preston, D. S., & Teubner, A. (2010). Information systems strategy: Reconceptualization, measurement, and implications. MIS Quarterly, 34(2), p.237.
[2] - Galliers, R. D. (1993). Towards a flexible information architecture: Integrating business strategies, information systems strategies, and business process redesign. (Definition cited in Allen, 1995).
[3] - Lederer, A. L., & Sethi, V. (1996). Toward a theory of strategic information systems planning. Journal of Strategic Information Systems, 5(3), 237–253.
[4] - Teubner, R. A. (2020). Understanding information systems strategy in the digital age: A review and research agenda. Journal of Strategic Information Systems, 29(4), 101642.

mainly as support for existing business models to studying how IS strategy co-drives digital transformation, innovation, and new value creation logics[1].

3.3. Organizational Structure and Design

Organizational structure and design describe how an organization arranges people, tasks, and decision rights, and how it deliberately shapes this arrangement to fit its strategy and environment. In academic work, they are treated as central determinants of coordination, control, information flows, and ultimately organizational performance[2].

3.3.1. Organizational structure

Organizational structure is usually defined as the relatively stable configuration of roles, responsibilities, authority relationships, and communication channels that governs how work is divided and coordinated. It specifies who reports to whom, how tasks are grouped into units, and how decisions and information move through the hierarchy and lateral linkages[3].

3.3.2. Organizational design

Organizational design refers to the intentional process of configuring structures, processes, and systems so that they align with the organization's strategy, environment, and technology. A dynamic, managerial activity involves choosing and adjusting structural forms, coordination mechanisms, and control systems to achieve strategic goals, efficiency, and adaptability.

3.3.3. Contingency and fit perspectives

Contingency theory argues that there is no single best structure; instead, effective design depends on contextual factors such as environment, size, technology, and strategy. High performance is expected when there is "fit" between structural arrangements and key contingencies, whereas misfit leads to coordination problems, inefficiencies, and lower performance.

3.3.4. Information processing and systems

Recent organization design research emphasizes that structure and design must match the organization's information-processing requirements arising from task interdependence and

[1] - Chen, D. Q., et al (2010), Op. Cit, p.679.
[2] - Galliers, R. D. (1993). Towards a flexible information architecture: Integrating business strategies, information systems strategies, and business process redesign. (Definition cited in Allen, 1995), p.102.
[3] - Teubner, R. A. (2020). Understanding information systems strategy in the digital age: A review and research agenda. Journal of Strategic Information Systems, 29(4), p.88.

environmental uncertainty. Information technology, including management information systems, both influences and is shaped by structure, as systems must adapt to centralized or decentralized designs and, conversely, can enable more flexible or integrated structural forms.

3.4. Fit and Congruence in Organization Theory

In organization theory, “fit” and “congruence” describe how well different elements of an organization (such as strategy, structure, processes, people, and environment) correspond to one another so that they function as a coherent, high-performing system[1]. These concepts are central in contingency and strategic management theories, which argue that effectiveness depends not on any single “best” design, but on the degree of alignment among key variables and contextual conditions.

3.4.1. Models Linking IS Strategy and Structure

Models linking information systems (IS) strategy and organizational structure explain how choices about technologies, applications, and IS roles must be coordinated with structural arrangements, governance, and value-creation logic to achieve alignment and performance[2].

These models share the assumption that IS strategy cannot be effective in isolation, but must “fit” both the competitive environment and the internal organization of work and authority. They provide lenses to analyze how portfolios, architectures, and processes IS reinforce or conflict with structural forms such as functional, divisional, or network organizations.

Three influential perspectives are the Strategic Alignment Model, information-intensity / value-chain views, and governance/decision-rights frameworks.

3.4.2. Strategic Alignment Model (SAM)

The Strategic Alignment Model (SAM) by Henderson and Venkatraman links business strategy, IS/IT strategy, organizational infrastructure and processes, and IS/IT infrastructure and processes in a four-domain framework. SAM posits that effectiveness depends on both “strategic fit” (consistency between external strategies and internal infrastructures) and “functional integration” (consistency between business and IS domains), highlighting explicit

[1] - Chen, D. Q., et al (2010), Op. Cit, p.679, p.282.

[2] -Galliers, R. D. (1993). Information systems strategy formation in higher education institutions. Information Research, 1(1).

alignment paths through which changes in strategy should drive adjustments in structure and IS architecture[1].

3.4.3. Information Intensity and Value Chain Perspectives

Information-intensity and value-chain perspectives emphasize how the information content of products and processes shapes appropriate IS strategies and structural designs. In industries or value-chain stages with high information intensity, organizations typically require more integrated, cross-functional IS architectures and coordination mechanisms[2], whereas low-intensity contexts may rely on more localized, functionally focused systems and structures.

3.4.4. Governance and Decision Rights in IS Strategy

Governance and decision-rights models focus on how authority over IS-related decisions (such as IT principles, architecture, infrastructure, and applications) is allocated across corporate, business-unit, and IT levels. This line of work shows that patterns of centralization or decentralization in IS governance need to be congruent with overall organizational structure and strategy, because misaligned decision-rights allocations lead to conflicts, shadow systems, and difficulties in executing IS strategy[3].

3.5. Patterns of Alignment and Misalignment

Alignment patterns refer to relatively stable combinations of business structure and IS arrangements such as centralized IT in a functional hierarchy or federated IT in a diversified group considered “fitting” given strategy and environment. Misalignment arises when IS governance, architecture, or services are configured in ways that conflict with structural requirements, creating tensions, redundancies, or coordination problems.

3.5.1. Centralized and Decentralized IS in Different Structures

In functional or highly centralized organizations, centralized IS units and standardized enterprise systems often support economies of scale and uniform processes, representing an aligned pattern. In divisional or multi-business structures, more decentralized or federated IS arrangements, sometimes coordinated through shared services or enterprise architecture standards, tend to fit better with local autonomy and differentiated strategies.

[1] - Henderson et al (1993), Op. Cit, p. 16.
[2] - Jordan, E. (1995). Information strategy: Alignment with organization structure. Journal of Strategic Information Systems, 4(4), 267–285.
[3] - Teubner, R. A. (2020). Understanding information systems strategy in the digital age. Journal of Strategic Information Systems, 29(4), 101642.

3.5.2. Structural Contingencies (divisional, matrix, network forms)

Divisional structures frequently rely on a mix of corporate-level platforms and divisional applications, while matrix and network forms require more lateral integration, shared data, and collaborative tools. Contingency-based work suggests that each structural form has a corresponding "ideal" IS configuration in terms of integration, standardization, and local flexibility, and that multiple effective configurations (equifinality) can exist when they jointly fit multiple contingencies such as environment and size[1].

3.5.3. Consequences of Misalignment

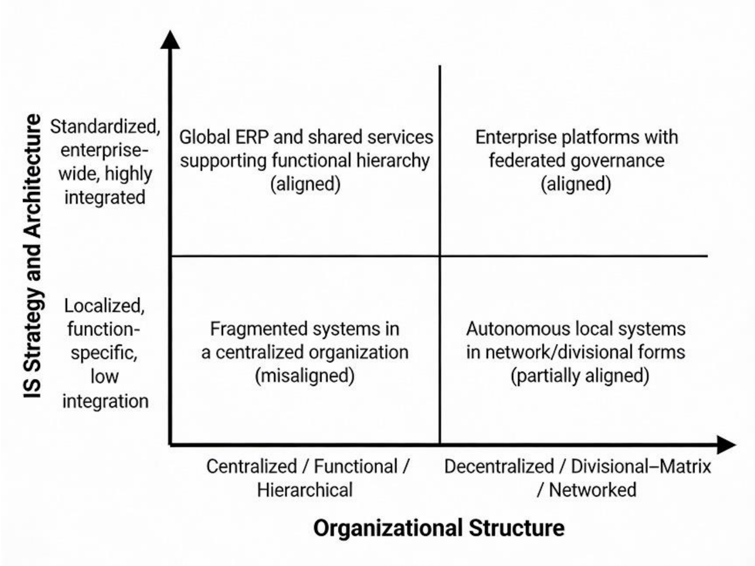
When IS centralization, architectures, or processes are inconsistent with structural demands such as highly centralized systems in a strongly entrepreneurial, networked organization, research reports increased shadow IT, duplication, slower decision-making, and user resistance[2]. Persistent misalignment can undermine strategic initiatives, inflate IT and coordination costs, and reduce the perceived value of IS, whereas aligned patterns are associated with smoother process integration, better information sharing, and improved performance[3].

3.6. IS Strategy, Digital Transformation, and Structural Change

Digital transformation research views IS strategy as a key lever for shifting organizations from traditional hierarchies and siloed processes to more integrated, data-driven, and ecosystem-oriented configurations[4]. Structural change is not just a consequence but also a prerequisite of effective IS strategy: new digital capabilities often demand redesigned roles, decision rights, and coordination mechanisms[5].

[1] - Donaldson, L. (2014). Fit – the key to organizational design. Journal of Organization Design, 3(3), 13–16.
[2] - Galliers, R. D. (1993). Information systems strategy formation in higher education institutions. Information Research, 1(1).
[3] - Pennings, J. M. (1992). Organizational structure and the use of information technology. International Journal of Information Management, 12(4), 284–298.
[4] - Jordan, E. (1995). Information strategy: Alignment with organization structure. Journal of Strategic Information Systems, 4(4), 267–285.
[5] - Njanka, S. Q., et al. (2021). IT–business alignment: A systematic literature review. Procedia Computer Science, 181, 803–810.

Figure 4.2: Alignment between IS Strategy and Organizational Structure



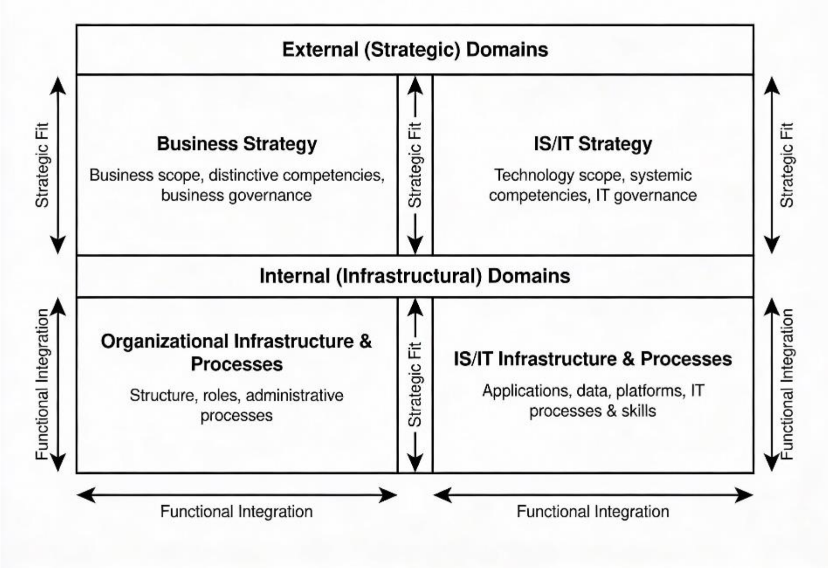
Source : (Jordan, 1995; Pennings, 1992; Teubner, 2020)

3.6.1. From Automation to Process Redesign and Business Scope Redefinition

Early uses of IT focused on automating existing tasks and processes, leaving underlying structures largely unchanged. Later work (for example, on business process reengineering) emphasizes using IS to fundamentally redesign processes, eliminate handoffs, and reconfigure organizational units around end-to-end value creation[1]. At the highest level, IS strategy can support "business scope redefinition," where firms use digital capabilities to enter new markets, create new services, or rethink their position in the value chain.

[1] - Jordan, E. (1995). Information strategy: Alignment with organization structure. Journal of Strategic Information Systems, 4(4), 267–285.

Figure 4.3: SAM-based View of IS Strategy and Organizational Infrastructure



Source: (Henderson & Venkatraman, 1993)

3.6.2. Platformization, Shared Services, and New Structural Forms

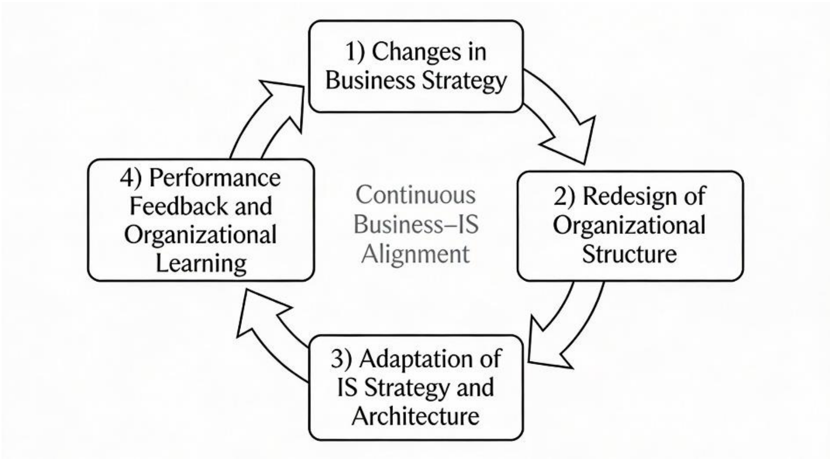
Digital transformation has accelerated “platformization,” where organizations build shared digital platforms and shared-services centers that provide standardized capabilities (such as data, integration, or analytics) to multiple business units[1]. These developments are associated with hybrid structural forms (for example, platform organizations, internal marketplaces, global business services) that decouple front-end business units from back-end shared digital infrastructure.

3.6.3. Dynamic Alignment in Turbulent Environments

In turbulent technological and market environments, IS strategy and structure must be continuously realigned rather than adjusted through occasional large-scale projects. Research highlights the need for dynamic capabilities such as agile governance, modular architectures, and iterative strategy processes that allow organizations to reconfigure structures and IS portfolios quickly as digital opportunities and threats evolve[2].

[1] - Shapiro, C et al (1999), Op. Cit, p.227.
[2] - Jordan, E. (1995). Information strategy: Alignment with organization structure. *Journal of Strategic Information Systems, 4*(4), 267–285.

Figure 4.4: Dynamic Alignment Loop



Source: (Njanka et al., 2021)

4. IT capabilities and competitive advantage

Information technology (IT) capabilities are widely analyzed through the resource-based view (RBV), which argues that certain internal resources can become sources of sustained competitive advantage when they are valuable, rare, difficult to imitate, and well organized. In this perspective, IT contributes to competitive advantage not simply through hardware and software, but through firm-specific capabilities that combine technology with people, processes, and organizational routines[1].

4.1. IT capabilities in the resource-based view

RBV-inspired IS research defines IT capability as a firm's ability to mobilize and deploy IT-based resources, such as infrastructure, human skills, and IT-enabled intangibles, in combination with other organizational resources. Empirical work shows that IT capabilities are multi-dimensional, typically encompassing IT infrastructure, IT human capability, and IT relationship (or managerial) capability, each contributing differently to value creation[2].

4.2. IT capability and firm performance

A seminal study by Bharadwaj conceptualizes IT capability as a higher-order construct arising from IT infrastructure, IT human resources, and IT-enabled intangibles, and finds that "IT-leader" firms with superior IT capabilities outperform matched control firms on several

[1] - Njanka, S. Q., et al. (2021). IT–business alignment: A systematic literature review. *Procedia Computer Science, 181*, 803–810.
[2] - Silvius, A. J. G. (2007). The strategic alignment of information systems strategy of public–private partnerships.

financial performance measures. Later studies and reviews broadly support a positive association between IT capability and firm performance, while also noting that the performance impact depends on complementarities with business processes, strategy, and organizational context[1].

4.3. From IT resources to competitive advantage

RBV and related work emphasize that IT resources yield competitive advantage when they satisfy VRIO criteria: they must be valuable (improving efficiency, quality, innovation, or responsiveness), rare (not widely possessed by competitors), difficult to imitate (for example, because they are embedded in complex socio-technical systems), and supported by appropriate organizational arrangements[2]. Reviews of ICT-related RBV applications highlight examples such as advanced analytics, IT-enabled supply-chain integration, strong IT–business relationships, and data-driven decision-making routines as IT-intensive capabilities that can differentiate firms in competitive markets.

4.4. Mechanisms linking IT capabilities to advantage

Information systems can support competitive advantage through multiple mechanisms, including cost reduction via process automation, differentiation through enhanced customer experience, faster and more informed decision-making, and the enablement of new products, services, or business models. Systematic reviews suggest that IT capabilities are especially powerful when they foster operational-level capabilities (such as process quality and flexibility) and innovation capabilities, thereby improving both efficiency and strategic adaptability[3].

[1] - Njanka, S. Q., et al. (2021). IT–business alignment: A systematic literature review. Procedia Computer Science, 181, 803–810.

[2] - Teubner, R. A. (2020). Understanding information systems strategy in the digital age. Journal of Strategic Information Systems, 29(4), 101642.

[3] - Teubner, R. A. (2020). Understanding information systems strategy in the digital age: A review and research agenda. Journal of Strategic Information Systems, 29(4), 101642.

5. Innovation and Digital Transformation

Innovation and digital transformation position Information Technology Management (ITM) as a strategic capability that reshapes business models, processes, and value propositions rather than merely supporting existing operations[1]. Contemporary literature stresses that sustained innovation requires an integrated approach to technology, strategy, governance, and culture, supported by structured innovation and transformation practices.

5.1. Role of ITM in driving innovation

ITM acts as an orchestrator of digital innovation by aligning technology roadmaps with business strategy, managing IT portfolios, and enabling experimentation with emerging technologies. Through practices such as innovation management, agile delivery, and platform governance, ITM helps organizations translate ideas into scalable digital products, services, and data-driven capabilities that enhance competitiveness and resilience[2].

5.2. Digital transformation frameworks and strategies

Digital transformation frameworks provide structured guidance for defining vision, prioritizing initiatives, and sequencing technology and organizational change, typically integrating dimensions such as strategy, customer experience, processes, technology, people, and governance[3]. Robust strategies emphasize clear leadership commitment, customer-centric design, data-driven decision-making, and iterative, agile implementation, supported by governance mechanisms, KPIs, and risk management practices to monitor and steer transformation outcomes.

5.3. Leveraging AI, IoT, and blockchain

Artificial Intelligence, the Internet of Things (IoT), and blockchain are frequently framed as key enablers of digital transformation because they extend organizational capabilities in analytics, automation, connectivity, and trust. AI enables predictive and prescriptive insights, IoT provides real-time data from connected assets and environments, and blockchain offers tamper-evident records and decentralized transaction mechanisms, together supporting new digital services, smarter operations, and more transparent, resilient value chains[4].

[1] - Chen, D. Q., et al (2010), Op. Cit, p.685.
[2] - Shapiro, C et al (1999), Op. Cit, p.289.
[3] - Reich, B. H., & Benbasat, I. (2000). Factors that influence the social dimension of alignment between business and information technology objectives. MIS Quarterly, 24(1), p.110.
[4] - Rizal, A., et al. (2025), Op. Cit, p.127.

5.4. Overcoming barriers to technological change

Research identifies recurrent barriers to technological change, including high implementation costs, legacy systems, skills gaps, cultural resistance, data privacy and cybersecurity concerns, and interoperability issues across heterogeneous platforms and partners[1]. Effective ITM responses combine change management and communication, workforce upskilling, incremental modernization of legacy landscapes, strong cybersecurity and data governance, and the adoption of open standards and modular architectures to ease integration and reduce transformation risk.

[1] - McAfee, A. et al (2012), Op. Cit, p.68.

CONCLUSION

Information Technology Management is presented as a strategic discipline that orchestrates technology, people, and processes so that digital resources systematically support and enhance organizational goals. It frames IT not as a background support function, but as a central mechanism through which firms pursue efficiency, innovation, and sustained competitive advantage in volatile environments. Over time, ITM has evolved from managing isolated technical infrastructures to governing integrated socio-technical systems that span hardware, software, networks, data, and human capabilities.

This historical trajectory from mainframe-based data processing, through the MIS and strategic IS eras, to contemporary cloud- and platform-based architectures illustrates how ITM has progressively shifted from operational automation to strategic value creation and organizational transformation. This evolution positions ITM at the heart of digital transformation, where strategic planning, governance frameworks, and risk management practices ensure that new technologies such as cloud computing, advanced analytics, and artificial intelligence are aligned with business priorities rather than adopted in an ad hoc, technology-driven manner. Through mechanisms like IT governance (COBIT, ITIL, ISO 27001), portfolio management, and enterprise architecture, ITM provides the structures and decision rights needed to translate technological possibilities into coherent roadmaps, measurable outcomes, and accountable ownership.

At the same time, effective ITM must navigate complex challenges, including escalating cybersecurity threats, fragmented and evolving regulatory regimes, organizational resistance to change, and persistent gaps between technical and business cultures. Addressing these tensions demands robust risk management, compliance capabilities, and deliberate change management strategies that foster trust, communication, and shared understanding across functional boundaries.

By embedding structured governance, continuous learning, and interdisciplinary coordination, ITM becomes a key driver of organizational resilience, enabling enterprises to adapt, innovate, and maintain performance in an increasingly digital, data-intensive world. In this sense, Information Technology Management is not merely about keeping systems running, but about shaping how organizations evolve, compete, and sustain value in the face of technological and environmental turbulence.

BOOKS

1. **Abdullah, Ojo & Martin, Saheed**. (2022). Risk Management Frameworks in Cybersecurity and Digital Investigations.

2. **Aitken, Lain** (2003), *Value-Driven IT Management*, ed. MPG Books Ltd, Bodmin, UK.

3. **Applegate, L. M., Austin, R. D., & McFarlan, F. W.** (2003). *Corporate Information Strategy and Management: Text and Cases* (6th ed.). McGraw-Hill.

4. **Barton, Robert** (2003), *Global IT Management*, ed. Wiley, London, England.

5. **Berebbia C.A** (2004), *Management Information Systems 2004, Fourth International Conference On Information Systems Incorporating GIS& Remote Sensing*, Wessex Institute of Technology, UK, editor WIT press, Southampton Boston, USA.

6. **Buchta Dirk, Eul Marcus** (2010), *Strategic IT Management – Increase value, control performance, reduce costs*, ed. Gabler, Wiesbaden, Germany.

7. **Bughin, J., et al.** (2018). *Notes from the AI frontier*. McKinsey Global Institute.

8. **Brown V. Carol, Sambaumurthy V.** (1999), *Repositioning the IT Organization to Enable Business Transformation*, Pinnanflex Educational Resources, Cincinnati, Ohio, USA.

9. **Ceruzzi, P. E.** (2003). *A History of Modern Computing* (2nd ed.). MIT Press.

10. **Chatham, Robina** (2015), *The Art of IT Management Practical tools, techniques and people skills*, ed. BCS Learning & Development Ltd, London, UK.

11. **COSO.** (2017). *Enterprise Risk Management—Integrating with Strategy and Performance*. Committee of Sponsoring Organizations of the Treadway Commission.
12. **De Mari, Guus** (2009), *Five Years of IT Management Improvement*, IOS Press, The Netherland.

13. **Dyché Jill** (2015), "*The New IT: How Technology Leaders Are Enabling Business Strategy in the Digital Age*", ed. McGraw-Hill Education, United States, 26.

14. **Ekman P., Dahlin P., Keller C.** (2002), *Management and Information Technology After Digital Information*, Routledge Studies in Innovation, Organization and Technology, New York, USA.

15. **Ekman, Peter & Co** (2022), *Management and Information Technology After Digital Transformation*, Routledge Taylor & Francis Group.

16. **Gallaugher, John**, *Information Systems, A Manager's Guide to Harnessing Technology*, ed. Flatwood, 2014, Boston, USA.

17. **Gartner** (2023). IT Infrastructure and Operations Management Market Guide.

18. **Gartner** (2022). Hype Cycle for IT Infrastructure and Operations.

19. **Greer, M., & Florwick, J.** (2021). IT Infrastructure & Operations: Managing in a Hybrid and Multi-Cloud World. O'Reilly Media.
20. **ISACA.** (2018). *COBIT 2019 Framework: Governance and Management Objectives*. Information Systems Audit and Control Association.

21. **Kelkar S.A** (2010), *Strategic IT Management – A Concise Study*, ed. PHI Learning Private Limited, New Delhi, India.

22. **Khan, M. Khaled, Zheng, Yan** (2005), *Managing Corporate Information Systems: Evolution and Maintenance*, ed. Idea Group Publishing, Sydney, Australia.

23. **Langer, Arthur M., Yorks, Lyle** (2018), *Strategic Information Technology Best Practices to Drive Digital Transformation* ed. Wiley, New Jersey, USA.

24. **Laudon Kenneth C, Laudon Jane P.** (2021), *Management Information Systems – Managing the Digital Firm*, Seventeenth (17°) edition, Pearson, United States.

25. **Lemberger Pirmin, Batty Marc**, *Big Data et Machine Learning, Les concepts et les outils de la Science Data*, ed. Dunod, 2019, Paris.

26. **McKenney, J. L.** (1995). *Waves of Change: Business Evolution through Information Technology*. Harvard Business School Press.

27. **Morgan, Tony** (2002), *Business Rules and Information Systems : Aligning IT with Business Goals*, Pearson education, Indianapolis, USA.

28. **Mc Kean, David** (2011), *IT Management*, ed. Ventus Publishing ApS, Oxfordshire, UK

29. **McKean, David** (2012), *IT Management, Part II Projects, Programs and Business Change*, ed. Bookboon, N-Y, USA.

30. **Narayanan V. K.** (2000), "*Managing Technology and Innovation for Competitive Advantage*", ed. Prentice Hall, United States.

31. **Porter, M. E.** (1985). *Competitive Advantage: Creating and Sustaining Superior Performance*. Free Press

32. **Piccoli, Gabriele** (2018), "*Information Systems for Managers*", ed. John Wiley & Sons, 4th edition, United States.

33. **Pilorget Lionel, Schell Thomas** (2018), *IT Management – The art of managing IT based on a solid framework leveraging the company's political ecosystem*, ed. Springer Vieweg, Wiesbaden, Germany.

34. **Savas Onur, Deng Julia** (2017), *Big Data Analytics in Cybersecurity*, CRC Press Taylor & Francis Group, New York – USA.

35. **Sisco, Mike** (2001), *IT Management -101 – Fundamentals to Archieve more*, ed. MDE.

36. **Sven Den Boer, Rajeev Andharia, Melvin Harteveld, Linh C Ho** (2006), *Six Sigma for IT Management*, ed. Van Haren Publishing, USA.

37. **Sparrow Elizabeth** (2003), *Successful IT Sourcing – From Choosing a Provider to Managing the Project*, ed. Springer, London, UK.

38. **University of Notre Dame**, Departement of Management (2010) *IT Management Applications*, ed. Pearson, Boston, USA.

39. **Urbach, Nils, Ahlemann, Frederick** (2019), *IT Management in Digital Age – A Roadmap for the IT Departement of the Future*, ed. Springer, Essen, Germany.

40. **Yorks, Lyle Langer, Arthur M.** (2013), *Best Practices for Managers and Excutives – Strategic IT*, ed. Wiley, New Jersey, USA.

41. **Weill, P., & Ross, J. W.** (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business School Press.

42. **Wilson, Frank** (2013), *IT Strategy made easy*, Kindel edition.

ARTICLES

1. **Alireza Nili, Colin Fidge, Michael Rosemann** (2024), *Why do project managers underuse Management Information Systems theories in their management of IT projects?*, Procedia Computer Science, Volume 239, 2024, Pages 1578-1585, ISSN 1877-0509. https://doi.org/10.1016/j.procs.2024.06.333.

2. **Ammann Jeanine, Walter Achim, El Benni Nadja** (2022), *Adoption and perception of farm management information systems by future Swiss farm managers – An online study*, Journal of Rural Studies, Volume 89, 2022, Pages 298-305, ISSN 0743-0167, https://doi.org/10.1016/j.jrurstud.2021.12.008.

3. **Armbrust, M., et al.** (2010). *A view of cloud computing*. Communications of the ACM, 53(4), 50–58. https://doi.org/10.1145/1721654.1721672.

4. **Arute, F., et al.** (2019). *Quantum supremacy using a programmable superconducting processor*. Nature, 574(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5.

5. **Atzori, L., Iera, A., & Morabito, G.** (2010). *The Internet of Things: A survey*. *Computer Networks*, 54(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

6. **Ayat, M., & Shafiee, S.** (2025). *Integrating COBIT 2019 and ISO/IEC 27001 for Strengthening IT Governance and Information Security*. Proceeding of the International Conference on Economics, Business, Science, and Technology. https://proceeding.raskhamedia.or.id/index.php/cessmuds/article/view/40

7. **Bacoș, I.B., Meruțiu, A., Gabor, M.R.** (2024). *Environmental Management System - Case Study on Citizens' Perception of Pollution at the Level of Mureș County. In: Moldovan, L., Gligor, A.* (eds) The 17th International Conference Interdisciplinarity in

Engineering. Inter-ENG 2023. Lecture Notes in Networks and Systems, vol 926. Springer, Cham. https://doi.org/10.1007/978-3-031-54664-8_38

8. **Barney, J.** (1991). *Firm Resources and Sustained Competitive Advantage. Journal of Management*, 17(1), 99–120. https://doi.org/10.1177/014920639101700108

9. **Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N.** (2013). *Digital Business Strategy: Toward a Next Generation of Insights. MIS Quarterly*, 37(2), 471–482.- https://doi.org/10.25300/MISQ/2013/37.2.08

10. **Blind, K., et al.** (2023). *Regulatory Fragmentation in the Digital Economy*. Journal of Policy Research.

11. **Bofan Song, Rongguang Liang** (2024), *Integrating Artificial Intelligence with Smartphone-based Imaging for Cancer Detection in vivo, Biosensors and Bioelectronic*, 116982, ISSN 0956-5663, https://doi.org/10.1016/j.bios.2024.116982.

12. **Brightlio.** (2025). *215 Data Center Stats (June-2025)*. Retrieved July 3, 2025, from https://brightlio.com/data-center-stats

13. **Byrd, T. A., & Turner, D. E.** (2001). *An exploratory examination of the relationship between flexible IT infrastructure and competitive advantage. Information & Management*, 39(1), 41–52. https://doi.org/10.1016/S0378-7206(01)00135-7

14. **Casino, F., Dasaklis, T. K., & Patsakis, C.** (2019). *A systematic literature review of blockchain-based applications.* Telematics and Informatics, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

15. **Chan, Y. E., Sabherwal, R., & Thatcher, J. B.** (2006). *Antecedents and outcomes of strategic IS alignment: An empirical investigation*. IEEE Transactions on Engineering Management, 53(1), 27–47. https://doi.org/10.1109/TEM.2005.861804

16. **Chen, I. J., & Popovich, K.** (2003). *Understanding customer relationship management (CRM). Business Process Management Journal*, 9(5), 672–688. https://doi.org/10.1108/14637150310496758

17. **Chen, H., Chiang, R. H., & Storey, V. C.** (2012). *Business intelligence and analytics: From big data to big impact.* MIS Quarterly, 36(4), 1165–1188. https://doi.org/10.2307/41703503

18. **Chui, M., Manyika, J., & Miremadi, M.** (2016). *Where machines could replace humans—and where they can't (yet).* McKinsey Quarterly. https://www.mckinsey.com/featured-insights/employment-and-growth/where-machines-could-replace-humans-and-where-they-cant-yet

19. **Cuenca, L., et al.** (2014). *The Role of Information Technology in Organizational Strategy*. Journal of Business Management.

20. **Davenport, T. H**. (1998). *Putting the enterprise into the enterprise system*. Harvard Business Review, 76(4), 121–131.

21. **Efe, Doç. Dr. Ahmet**. (2023). A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT.

22. **Efe, A.** (2023). *A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT*. *Journal of Auditing and Assurance Services*, *3*(2).

23. **Floridi, L., & Cowls, J.** (2019). A unified framework of five principles for AI in society. Harvard Data Science Review.

24. **Henderson, J. C., & Venkatraman, N.** (1993). *Strategic alignment: Leveraging information technology for transforming organizations*. *IBM Systems Journal*, 32(1), 4–16.

25. **Hammer, M., & Champy, J.** (1993). Reengineering the Corporation: A Manifesto for Business Revolution. From : Magazine (July–August 1990) https://hbr.org/1990/07/reengineering-work-dont-automate-obliterate

26. **Henderson, J. C., & Venkatraman, N.** (1993). Strategic alignment: Leveraging information technology for transforming organizations. IBM Systems Journal, 32(1), 4–16. https://doi.org/10.1147/sj.382.0472

27. **Hendry Naufal Marbella, Izzat Aulia Akbar, Bambang Setiawan** (2024), *Design and development of a web-based patient management information system*, Procedia Computer Science, Volume 234, 2024, Pages 1799-1806, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.03.188.

28. **Gulzar, Maryam** (2023*), IT Infrastructure Management: A Digital Services Context*, LUT University, Yliopistonkatu 34, 53850 Lappeenranta, Finland. accessed July 21, 2025 https://ceur-ws.org/Vol-3621/phd-paper6.pdf

29. **GDPR.** (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council*. Official Journal of the European Union.

30. **Kaplan, A. M., & Haenlein, M.** (2010). *Users of the world, unite! The challenges and opportunities of social media*. *Business Horizons*, 53(1), 59–68.

31. **Kappelman, L., McLean, E., Johnson, V., & Torres, R.** (2019). The 2019 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, 18(1), 1–20.

32. **Karydas Christos, Chatziantoniou Myrto, Stamkopoulos Kostas, Iatrou Miltiadis, Vassiliadis Vangelis, Mourelatos Spiros,** (2023), *Embedding a precision agriculture service into a farm management information system - ifarma/PreFer, Smart Agricultural Technology*, Volume 4,2023, 100175, ISSN 2772-3755. https://doi.org/10.1016/j.atech.2023.100175.

33. **Karahanna, E., & Preston, D. S.** (2013). The Effect of Social Capital of the Relationship Between the CIO and Top Management Team on Firm Performance. Journal of Management Information Systems.

34. **Kopperapu, R.** (2024). *Regulatory Frameworks and Compliance Strategies for Protecting Consumer Data*. ResearchGate.

35. **Leego, E., & Bider, I.** (2023). *Aligning ISO 27001 with Business Objectives: A governance perspective*. Journal of Systems and Software.

36. **Loeser, F., Erek, K., & Zarnekow, R.** (2017). *Aligning IT with sustainability goals: Design patterns for sustainable IT governance*. Communications of the Association for Information Systems, 41, Article 24.

37. **Luftman, J.** (2015). Assessing Business-IT Alignment Maturity. *Communications of the Association for Information Systems*.

38. **Luftman, J., Kempaiah, R., & Nash, E.** (2004). *Key issues for IT executives 2004. MIS Quarterly Executive*, 3(2), 89–104.

39. **Luftman, J., & Kempaiah, R.** (2007). *An Update on Business-IT Alignment: A Line Has Been Drawn. MIS Quarterly Executive*, 6(3), 165–177. https://doi.org/10.17705/1CAIS.00414

40. **Luftman, J.** (2000). *Assessing business-IT alignment maturity. Communications of the Association for Information Systems*, 4(14).

41. **McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D.** (2012). *Big data: The management revolution. Harvard Business Review*, 90(10), 60–68.

42. **Melaku, B.** (2023). *Barriers to Effective IT Governance in Developing Economies*. African Journal of Information Systems.

43. **Melzer, Marvin, Bellingrath-Kimura, Sonoko; Gandorfer, Markus** (2023), *Commercial farm management information systems - A demand-oriented analysis of functions in practical use, Smart Agricultural Technology*, Volume 4, 2023, 100203, ISSN 2772-3755, https://doi.org/10.1016/j.atech.2023.100203.

44. **Metin, B., et al.** (2024). *IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture*. *Information*, *15*(1), 55.

45. **Muhammad Arslan, Zainab Riaz, Christophe Cruz** (2023), *Revolutionizing Management Information Systems with Natural Language Processing for Digital Transformation*, Procedia Computer Science, Volume 225, 2023, Pages 2835-2844, https://doi.org/10.1016/j.procs.2023.10.276.

46. **Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M.** (2017). *Digital innovation management: Reinventing innovation management research in a digital world*. *MIS Quarterly*, 41(1), 223–238.

47. **Nespeca V., T. Comes, K. Meesters, F. Brazier** (2020), *Towards coordinated self-organization: An actor-centered framework for the design of disaster management information systems*, International Journal of Disaster Risk Reduction, Volume 51, 2020, ISSN 2212-4209, https://doi.org/10.1016/j.ijdrr.2020.101887.

48. **NIST.** (2018). *NIST Special Publication 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations*. National Institute of Standards and Technology.

49. **Peppard, J., & Ward, J.** (2004). *Beyond strategic information systems: towards an IS capability. Journal of Strategic Information Systems*, 13(2), 167–194. https://doi.org/10.1016/j.jsis.2004.02.002

50. **Pingbo Qu** (2024), *Design of Supply Chain Logistics Intelligent Management Information System Based on GIS Optimization Model*, Procedia Computer Science, Volume 243, 2024, Pages 396-405, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.09.049.

51. **Porter, M. E.** (1996). *What is strategy?* Harvard Business Review, 74(6), 61–78. https://hbr.org/1996/11/what-is-strategy

52. **Protiviti.** (2025). *Top compliance challenges facing the technology industry in 2025*. Protiviti Global.

53. **Reich, B. H., & Benbasat, I.** (2000). *Factors that influence the social dimension of alignment between business and information technology objectives*. MIS Quarterly, 24(1), 81–113. https://doi.org/10.2307/3250980

54. **Rippling.** (2025). *What Is IT Compliance? Risks, Best Practices, & Checklist (2025)*. Rippling Blog.

55. **Rizal, A., et al.** (2025). *Challenges in Harmonizing IT Governance Frameworks: A Case Study of COBIT and ISO Standards*. International Journal of Information Management.

56. **Shapiro, C., & Varian, H. R.** (1999). Information Rules: A Strategic Guide to the Network Economy. Harvard Business School Press.

57. **Senna P, da Cunha Reis A, Castro A, Dias AC** (2020), *Promising research fields in supply chain risk management and supply chain resilience and the gaps concerning human factors: A literature review*. Work. 2020;67(2):487-498. https://doi.org/10.3233/WOR-203298. PMID: 33074212.

58. **Shi, W., et al.** (2016)**,** *Edge computing: Vision and challenges*. IEEE Internet of Things Journal, 3(5), 637–646.

59. **Simon, H. A.** (1976). *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization* (3rd ed.). Free Press.

60. **Sudarat Srima, Panita Wannapiroon, Prachyanun Nilsook** (2015), *Design of Total Quality Management Information System (TQMIS) for Model School on Best Practice, Procedia - Social and Behavioral Sciences*, Volume 174, 2015, Pages 2160-2165, ISSN 1877-0428, https://doi.org/10.1016/j.sbspro.2015.02.016.

61. **Swapan Basu** (2024), *Chapter 14 - Management information system (MIS), Editor(s): Swapan Basu, Plant Intelligent Automation and Digital Transformation*, Academic

Press, 2024, Pages 397-415, ISBN 9780128244579, https://doi.org/10.1016/B978-0-12-824457-9.00018-2.

62. **Tallon, P. P., & Pinsonneault, A.** (2011). *Competing perspectives on the link between strategic information technology alignment and organizational agility: Insights from a mediation model*. MIS Quarterly, 35(2), 463–486.

63. **Taherdoost Hamed, Madanchian Mitra** (2022), *Employment of Technological-Based Approaches for Creative E-Learning; Teaching Management Information Systems*, Procedia Computer Science, Volume 215, 2022, Pages 802-808, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.12.082.

64. **Tsiu, T., et al.** (2024). *The Impact of IT Strategic Planning Process on SME Performance: A Systematic Review*. MDPI, Journal of Open Innovation.

65. **Vial Gregory** (2019), *Understanding digital transformation: A review and a research agenda*, The Journal of Strategic Information Systems, Volume 28, Issue 2, 2019, Pages 118-144, ISSN 0963-8687, https://doi.org/10.1016/j.jsis.2019.01.003.

66. **Von Solms, R., & Van Niekerk, J.** (2013). *From information security to cybersecurity*. *Computers & Security*, 38, 97–102.

67. **Wade, M., & Hulland, J.** (2004). *Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research*. MIS Quarterly, 28(1), 107–142. https://doi.org/10.2307/25148626

68. **Wang, T., et al.** (2024). *A Survey of Major Cybersecurity Compliance Frameworks*. Proceedings of the IEEE International Conference on Cyber Security and Resilience.

69. **Weill, P., & Broadbent, M.** (1998). *Leveraging the New Infrastructure: How Market Leaders Capitalize on Information Technology*. Harvard Business School Press. https://hbr.org/product/leveraging-the-new-infrastructure-how-market-leaders-capitalize-on-information-technology/2706-HBK-ENG

70. **West, J., & Mace, M.** (2010). *Browsing as the killer app: Explaining the rapid success of Apple's iPhone*. Telecommunications Policy, 34(5–6), 270–286.

71. **Xiaoming Zhang, Shina Qiao, Rongrong Zhang, Minjun Liu, Lili Wu, Hongying Pan** (2023), *Construction and Application of Chain Management Information System for Cancer Pain*, Pain Management Nursing, Volume 24, Issue 4, 2023, Pages e75-e80, ISSN 1524-9042, https://doi.org/10.1016/j.pmn.2023.04.004.

72. **Zhao, Y., Fan, S., & Hu, D.** (2021). The evolution of enterprise system integration: A literature review. *Information Systems Frontiers*, 23, 627–652.

ABREVIATION

CIO: Chief Information Officer
IS : Information Systems
ITM: Information Technology Management
PC/PCs: Personal Computer(s)
POS: Point of Sale (term used in examples of embedded/IoT clients)
AIOps : Artificial Intelligence Opetations
AIOps: Artificial Intelligence for IT Operations
BCDR: Business Continuity and Disaster Recovery
BCMS: Business Continuity Management System
BI: Business Intelligence
BITA: Business–IT Alignment
CCPA: California Consumer Privacy Act
COBIT: Control Objectives for Information and Related Technologies
COSO ERM: Committee of Sponsoring Organizations Enterprise Risk Management
CRM: Customer Relationship Management
DBMS: Database Management System
ERP: Enterprise Resource Planning
GDPR: General Data Protection Regulation
HCM/HRM: Human Capital Management / Human Resource Management
HIPAA: Health Insurance Portability and Accountability Act
I&O units : Input/Output units
IoT: Internet of Things
ISMS: Information Security Management System
ISO 27005: Information Security Risk Management standard
ISO 31000: Enterprise Risk Management standard
ISO/IEC 27001: Information Security Management System standard (ISMS)
ITGCs: IT General Controls
ITIL : Information Technology Infrastructure Library
ITIL: Information Technology Infrastructure Library
ITSM: IT Service Management
KPI / KPIs: Key Performance Indicator(s)
LAN: Local Area Network
MDM: Mobile Device Management
MPLS: Multi-Protocol Label Switching
NIST CSF: NIST Cybersecurity Framework
NIST RMF: NIST Risk Management Framework
NIST: National Institute of Standards and Technology
OS : Operating System
OS : Operating System
PCI DSS: Payment Card Industry Data Security Standard
PHI / ePHI: (Electronic) Protected Health Information
PI: Personal Information (or Personal Data)
PIPL: Personal Information Protection Law (China)
RBV: Resource-Based View
RegTech: Regulatory Technology
ROI: Return on Investment
RPO: Recovery Point Objective

RTO: Recovery Time Objective
SaaS: Software as a Service
SAM: Strategic Alignment Model
SASE: Secure Access Service Edge
SCM: Supply Chain Management
SDN: Software-Defined Networking
SD-WAN / SDWAN: Software-Defined Wide Area Network
SD-WAN: Software-Defined Wide Area Network
SIS : Strategic Information Systems
SOX: Sarbanes–Oxley Act
UCC: Unified Communications and Collaboration
VDI: Virtual Desktop Infrastructure
VoIP: Voice over IP
VPN: Virtual Private Network
VRIN: Valuable, Rare, Inimitable, Non-substitutable
WAN: Wide Area Network
WiFi: Wireless Fidelity