



Akademik Eğitim ve Sosyal Bilimler Dergisi (AJESS Journal)

Integrating Digital Transformation and Risk Management: Comparative Evidence from Saudi Arabia's Energy, Industrial, and Telecommunications Sectors

Dijital Dönüşüm ile Risk Yönetiminin Bütünleştirilmesi: Suudi Arabistan'ın Enerji, Sanayi ve Telekomünikasyon Sektörlerinden Karşılaştırmalı Bulgular

Nabila Makhoulf

Mohamed Khider University of Biskra, Algeria

Email: nabila.makhoulf@univ-biskra.dz

ORCID: <https://orcid.org/0009-0000-5298-5348>

Hanane Maalla

Martyr Hama Lakhdar University of El Oued, Algeria

Email: maalla-hanane@univ-eloued.dz

ORCID: <https://orcid.org/0009-0008-4759-4367>

Youssera Djehiche

University of Algiers 3, Algeria

Email: djehiche.youssera@univ-alger3.dz

ORCID: <https://orcid.org/0009-0005-0518-4384>

Received: April 22, 2025

Accepted: March 2, 2026

Published Online: August 2, 2026

Abstract

Digital transformation is reshaping risk management by enabling organizations to move from reactive responses toward proactive, data-driven, and predictive decision-making. This study examines how digital transformation has contributed to the development of risk-management methodologies in three major Saudi companies operating in distinct sectors: Saudi Aramco in energy, SABIC in industry, and stc in telecommunications. The research employs a descriptive-analytical design for the theoretical component and a comparative multiple-case-study approach for the empirical component. Publicly available company materials and relevant secondary sources relating to the 2024 reporting period are analyzed to identify shared strategic objectives, sector-specific risk profiles, digital technologies, and implementation patterns. The findings indicate that all three companies seek to improve risk anticipation, operational resilience, business continuity, and decision quality. However, the technologies prioritized by each organization vary

Türkçe Öz

Dijital dönüşüm, kuruluşların risklere tepki veren geleneksel yaklaşımlardan proaktif, veriye dayalı ve öngörücü karar alma modellerine geçmesini sağlayarak risk yönetimini yeniden şekillendirmektedir. Bu çalışma, dijital dönüşümün farklı sektörlerde faaliyet gösteren üç büyük Suudi şirketindeki risk yönetimi yöntemlerinin gelişimine katkısını incelemektedir: enerji sektöründe Saudi Aramco, sanayi sektöründe SABIC ve telekomünikasyon sektöründe stc. Araştırmacının kuramsal bölümünde betimleyici-analitik desen, uygulamalı bölümünde ise karşılaştırmalı çoklu durum çalışması yaklaşımı kullanılmıştır. Ortak stratejik amaçları, sektöre özgü risk profillerini, dijital teknolojileri ve uygulama modellerini belirlemek amacıyla şirketlerin kamuya açık kurumsal materyalleri ile 2024 raporlama dönemine ilişkin ikincil kaynaklar incelenmiştir. Bulgular, üç şirketin de riskleri önceden belirlemeyi, operasyonel dayanıklılığı, iş sürekliliğini ve karar kalitesini geliştirmeyi amaçladığını

Cited For: Makhoulf, N., Maalla, H., & Djehiche, Y. (2026). Integrating Digital Transformation and Risk Management: Comparative Evidence from Saudi Arabia's Energy, Industrial, and Telecommunications Sectors. *Akademik Eğitim ve Sosyal Bilimler Dergisi (AJESS Journal)*, 3, Article e26.

according to its principal vulnerabilities and operating environment. The analysis further suggests that successful integration is not determined solely by technological sophistication or investment scale. Its effectiveness depends more fundamentally on the alignment of digital capabilities with material risk exposures, governance arrangements, organizational processes, and data quality. Artificial intelligence, automation, advanced analytics, and digital monitoring generate value when embedded within a coherent risk-governance framework. The study concludes that organizations should prioritize high-impact vulnerabilities, strengthen data governance, establish clear accountability, and evaluate digital solutions according to measurable risk outcomes. These findings provide a sector-sensitive framework for organizations seeking to develop predictive and resilient risk-management systems. Keywords: digital transformation; enterprise risk management; artificial intelligence; predictive analytics; organizational resilience; Saudi Arabia	göstermektedir. Bununla birlikte her kuruluşun öncelik verdiği teknolojiler, karşılaştığı temel kırılganlıklara ve faaliyet ortamına göre farklılaşmaktadır. Analiz ayrıca başarılı bir bütünleşmenin yalnızca teknolojik gelişmişlik düzeyine veya yatırım ölçeğine bağlı olmadığını göstermektedir. Etkililik daha çok dijital kabiliyetlerin önemli risklerle, yönetim düzenlemeleriyle, kurumsal süreçlerle ve veri kalitesiyle uyumuna bağlıdır. Yapay zekâ, otomasyon, ileri analitik ve dijital izleme sistemleri, bütüncül bir risk yönetimi çerçevesine yerleştirildiğinde değer üretmektedir. Çalışma, kuruluşların yüksek etkili kırılganlıklara öncelik vermesini, veri yönetimini güçlendirmesini, sorumlulukları açıkça belirlemesini ve dijital çözümleri ölçülebilir risk sonuçlarına göre değerlendirmesini önermektedir. Anahtar Kelimeler: dijital dönüşüm; kurumsal risk yönetimi; yapay zekâ; öngörücü analitik; kurumsal dayanıklılık; Suudi Arabistan
---	---

Introduction

Digital transformation has become a strategic requirement for organizations seeking to maintain competitiveness, operational continuity, and resilience in increasingly uncertain business environments. Developments in artificial intelligence, automation, cloud infrastructure, the Internet of Things, advanced analytics, and real-time monitoring have changed how organizations collect information, coordinate operations, and make decisions. These technologies are no longer used solely to improve efficiency or reduce costs. They increasingly influence organizational governance, strategic planning, compliance, security, and risk management.

Traditional risk-management systems have generally relied on historical information, periodic assessments, predetermined risk registers, and responses initiated after a threat has materialized. Although these practices remain important, they may be insufficient in environments characterized by rapid technological change, interconnected supply chains, volatile markets, cyber threats, environmental pressures, and operational complexity. Contemporary organizations therefore face growing pressure to supplement reactive controls with proactive and predictive capabilities.

The integration of digital transformation and risk management addresses this requirement by using data and technology to identify emerging threats, detect anomalies, model possible scenarios, and support earlier intervention. Artificial intelligence and machine-learning applications may identify patterns that conventional analysis cannot easily detect. Automation can reduce process variability and strengthen the consistency of controls. Digital monitoring systems can provide continuous information about infrastructure, equipment, networks, and operational conditions. Advanced analytics can support scenario analysis, forecasting, resource allocation, and management decisions.

Nevertheless, the adoption of advanced technology does not automatically produce effective risk management. Digital initiatives may generate new vulnerabilities, including cyber exposure, data-quality problems, algorithmic bias, dependence on complex technological systems, integration difficulties, and unclear accountability. Technology can therefore operate simultaneously as a risk-management instrument and a source of new risk. This dual effect requires organizations to align digital transformation with governance structures, organizational capabilities, sectoral requirements, and clearly defined risk priorities.

Sectoral context is particularly important in this alignment. Energy companies operate complex physical assets and critical infrastructure and must address operational safety, production continuity, environmental exposure, and market volatility. Industrial companies manage manufacturing systems, supply chains, equipment reliability, product quality, occupational safety, and resource efficiency. Telecommunications companies face network availability, cybersecurity, data protection, service continuity, customer demand, and rapid technological obsolescence. Although these sectors may use similar technologies, the purpose, configuration, and expected outcomes of their digital applications can differ substantially.

Saudi Arabia offers a relevant setting for examining these differences. The country's economic transformation has increased the strategic importance of digitalization, innovation, operational resilience, and effective corporate governance. Saudi Aramco, SABIC, and stc represent major organizations in the energy, industrial, and telecommunications sectors, respectively. Their scale, strategic importance, and distinct risk environments provide an appropriate basis for comparative analysis.

Despite the increasing literature on digital transformation and enterprise risk management, these subjects are frequently examined separately. Digital-transformation studies often emphasize innovation, productivity, and customer value, while risk-management research focuses on governance, compliance, controls, and business continuity. This separation limits understanding of how digital technologies alter risk identification, assessment, monitoring, mitigation, and reporting. Comparative evidence across sectors is also relatively limited, particularly regarding how organizations select technologies in response to different risk profiles.

This study addresses this gap by examining how Saudi Aramco, SABIC, and stc integrate digital capabilities into their risk-management approaches. Its central research question is: How has the integration of digital transformation contributed to the development of risk-management methodologies in major Saudi companies?

Two supporting questions guide the analysis. First, which strategic objectives are shared by the three companies when integrating digital transformation with risk management? Second, how do their technology choices differ according to the risks associated with the energy, industrial, and telecommunications sectors?

The study advances two propositions. The first is that the principal shared objective of integration is a transition from reactive risk management toward proactive and predictive management. The second is that sector-specific risk profiles lead companies to prioritize different combinations of digital technologies, even when the broad categories of technology are similar.

Accordingly, the study aims to clarify the conceptual relationship between digital transformation and risk management; identify shared and sector-specific strategic objectives; compare the digital technologies employed across the selected companies; analyze the alignment between technological capabilities and material risk exposures; and develop practical recommendations for organizations seeking to strengthen digital risk-management strategies.

The study contributes to the literature in three respects. Conceptually, it connects digital transformation with the development of predictive risk-management capabilities. Empirically, it provides a cross-sector comparison involving three strategically important Saudi companies. Managerially, it emphasizes that effective digital risk management depends less on acquiring the most sophisticated technology than on selecting solutions that address material vulnerabilities, operate on reliable data, and are embedded within coherent governance and decision-making processes.

Methodology

Research Design

This study adopts a qualitative, descriptive-analytical research design combined with a comparative multiple-case-study approach. The descriptive-analytical component establishes the conceptual relationship between digital transformation and enterprise risk management, while the multiple-case design examines how this relationship is operationalized in three major Saudi companies: Saudi Aramco, SABIC, and stc.

The comparative approach is appropriate because the selected organizations operate in sectors with substantially different risk profiles. Saudi Aramco represents the energy sector, SABIC represents the petrochemical and industrial sector, and stc represents telecommunications and digital services. Comparing these cases makes it possible to distinguish common integration principles from sector-specific technological responses.

Research Questions and Propositions

The study addresses the following central question:

How has the integration of digital transformation contributed to the development of risk-management methodologies in Saudi Aramco, SABIC, and stc?

The analysis is guided by two supporting questions:

- Which strategic objectives are shared by the three companies when integrating digital transformation with risk management?
- How do the technologies prioritized by each company differ according to its sector-specific risk exposures?

Two analytical propositions structure the comparison. The first proposes that the shared objective of integration is to move from reactive risk management toward proactive, continuous, and predictive risk management. The second proposes that variation in sectoral risk profiles leads organizations to adopt different configurations of artificial intelligence, automation, advanced analytics, and digital monitoring technologies.

These propositions serve as analytical expectations rather than hypotheses tested through inferential statistics.

Case Selection

The cases were selected purposively through a maximum-variation logic. Three criteria guided the selection. First, each company holds substantial strategic and economic importance within Saudi Arabia. Second, the companies operate in sectors characterized by different combinations of operational, technological, financial, strategic, regulatory, safety, and cybersecurity risks. Third, each organization publicly reports information concerning enterprise risk management, governance, digital transformation, data, innovation, or technological development.

The selection enables a structured comparison across heterogeneous operating environments. Saudi Aramco's risk environment is associated principally with energy infrastructure, asset integrity, production continuity, market exposure, safety, and environmental performance. SABIC operates within a complex industrial and petrochemical environment involving manufacturing, supply chains, regulatory compliance, process safety, and market cyclicality. stc is exposed particularly to network continuity, cybersecurity, data protection, digital-service reliability, technological change, and customer-related risks.

The cases are not intended to statistically represent all Saudi companies. They are used to support analytical generalization by identifying mechanisms and patterns that may be relevant to other large organizations operating in technology-intensive sectors.

Temporal Scope

The principal period of analysis is the 2024 reporting year. A common reporting period was selected to improve comparability among the cases and reduce distortions caused by different economic or technological conditions. Earlier sources were used only to clarify theoretical concepts, historical developments, or initiatives whose effects continued into 2024.

The study therefore provides a cross-sectional comparison of publicly reported practices rather than a longitudinal evaluation of organizational change.

Data Sources

The study relies on secondary documentary evidence. The principal sources consist of the companies' 2024 annual or integrated reports, publicly available risk-management disclosures, governance information, sustainability materials, and official descriptions of digital-transformation initiatives. Relevant academic studies, professional reports, and recognized risk-management literature are used to develop the theoretical framework and support interpretation.

Company-generated sources are treated as official organizational disclosures rather than independent evaluations of performance. Statements concerning the objectives or benefits of digital initiatives are therefore distinguished from externally verified evidence of their outcomes.

Documents were included when they contained information concerning at least one of the following areas:

- Enterprise risk-management governance and responsibilities;

- Risk-identification, assessment, monitoring, or reporting processes;
- Principal strategic, operational, financial, compliance, technological, or sustainability risks;
- Artificial intelligence, automation, advanced analytics, digital monitoring, or data infrastructure;
- Business continuity, resilience, cybersecurity, asset reliability, or predictive maintenance;
- Data governance, digital skills, or organizational capabilities supporting technology adoption;
- Evidence connecting a digital initiative with a specific risk-management function.

Documents that mentioned innovation or digitalization without identifying an organizational objective, technological capability, risk category, or relevant application were excluded from the main comparison.

Unit of Analysis

The primary unit of analysis is the **digital risk-management practice**. This refers to a documented organizational arrangement, technological capability, or operational initiative through which digital transformation contributes to the identification, assessment, monitoring, mitigation, communication, or governance of risk.

Examples include the use of predictive analytics to anticipate equipment failure, automated monitoring to detect operational anomalies, artificial intelligence to support forecasting, digital platforms to strengthen enterprise-wide risk reporting, and data-governance measures intended to improve the reliability of risk information.

The company constitutes the embedded case, while individual digital risk-management practices constitute the units examined within each case.

Data Extraction and Coding Framework

Relevant information was extracted using a structured analytical matrix to ensure that the same criteria were applied to all three companies. The matrix contains the following dimensions:

Table 2. Analytical Framework for the Cross-Case Evaluation of Digital Transformation and Risk-Management Integration

Analytical dimension	Information examined
Sector context	Business model, operational environment, and critical assets
Risk profile	Strategic, operational, financial, compliance, cyber, safety, and sustainability risks
Strategic objective	Resilience, continuity, forecasting, efficiency, compliance, or decision quality
Digital technology	Artificial intelligence, automation, analytics, digital monitoring, or integrated platforms
Risk-management function	Identification, assessment, prediction, monitoring, mitigation, reporting, or response
Governance enabler	Accountability, policies, controls, risk appetite, and management oversight
Data enabler	Data quality, integration, accessibility, security, and governance
Human capability	Digital skills, training, organizational learning, and cross-functional coordination
Reported outcome	Early warning, predictive capacity, reduced disruption, improved control, or stronger resilience
Implementation constraint	Cyber exposure, legacy systems, data limitations, skills gaps, or integration complexity

The coding framework combines deductive and inductive logic. Deductive categories were derived from the literature on digital transformation and enterprise risk management. Additional subthemes were developed inductively when recurring patterns emerged from the company materials.

Analytical Procedure

The analysis was conducted in two stages. The first involved within-case analysis. Each company was examined independently to identify its risk-governance framework, material risk categories, digital-transformation priorities, technological applications, and reported links between digital capabilities and risk-management processes. This stage preserved the sectoral and organizational context of each case.

The second stage involved cross-case synthesis. Findings from the three cases were entered into a common comparison matrix and examined for similarities, differences, and recurring relationships. Common patterns included the transition toward early warning, continuous monitoring, predictive analysis, organizational resilience, and data-driven decision-making. Differences were analyzed in relation to sector-specific vulnerabilities and operational requirements.

Pattern matching was used to assess the study's propositions. Evidence showing that the three companies emphasized anticipation, prediction, or early intervention was compared with the first proposition. Differences in technology selection and application were compared with the second proposition concerning sectoral risk profiles.

The study does not infer causality merely from the simultaneous presence of digital technologies and improved risk-management objectives. A relationship was interpreted cautiously and only when company disclosures or supporting evidence explicitly connected a technology with a particular risk-management function.

Comparative Logic

The comparison distinguishes between technological similarity and functional equivalence. The same technology may serve different purposes in different sectors. For example, artificial intelligence may support equipment reliability in energy operations, process optimization in industrial production, and network monitoring in telecommunications. Conversely, different technologies may perform equivalent risk-management functions, such as early detection or continuity protection.

This distinction enables the study to evaluate alignment rather than technological sophistication alone. Integration is considered stronger when the selected technology addresses a clearly defined material risk, operates within an established governance framework, relies on sufficiently reliable data, and contributes to a specified risk-management function.

Trustworthiness and Analytical Rigor

Several procedures were incorporated to strengthen the credibility of the analysis. A common extraction framework was applied across all cases, and claims were checked against more than one document where equivalent evidence was available. Company statements were compared with relevant academic and professional literature to reduce dependence on corporate self-presentation.

A transparent chain of evidence was maintained by linking each interpretation to its documentary source, reporting year, and relevant page or section. Conceptual definitions were applied consistently, particularly when distinguishing digital transformation, routine information technology, and digitally enabled risk management.

Negative or incomplete evidence was not interpreted as proof that a practice did not exist. Because corporate reports vary in detail, the absence of disclosure was recorded as “not identified in the reviewed documents” rather than “not implemented.”

Ethical Considerations

The study uses publicly available corporate and scholarly documents and does not involve human participants, confidential company information, personal data, interviews, or experimental procedures. Ethics committee approval and informed consent were therefore not required. All documentary and conceptual sources should be cited accurately.

Methodological Limitations

The methodology has several limitations. Corporate reports are prepared partly for accountability and reputation purposes and may emphasize achievements more strongly than implementation failures. The study is consequently dependent on what the companies chose to disclose publicly.

The use of a single reporting year limits the ability to assess change over time or establish whether reported initiatives produced sustainable outcomes. The three cases also differ in organizational scale, regulatory environment, and disclosure practices, which constrains direct comparison.

The study does not use internal performance data, interviews with risk managers, cybersecurity specialists, or digital-transformation executives. It therefore cannot independently verify operational effectiveness or quantify causal effects. Reported benefits should be interpreted as documentary evidence of organizational practices and strategic orientation rather than as experimentally validated performance improvements.

Future research could address these limitations through longitudinal analysis, interviews, internal risk indicators, maturity assessments, and quantitative measures linking digital investments with operational resilience, incident frequency, forecasting accuracy, or business-continuity outcomes.

Results and Discussion

The cross-case analysis identified a common strategic direction across SABIC, Saudi Aramco, and stc: the use of digital transformation to move risk management from periodic and reactive control toward continuous, proactive, and increasingly predictive management. Nevertheless, the technologies, implementation priorities, and risk-management functions differed substantially according to each company’s sectoral exposure.

Risk Governance as the Foundation of Digital Integration

The first finding is that digital risk management in all three cases is embedded within broader enterprise risk-management and governance arrangements. Digital technologies are not presented as independent substitutes for conventional risk controls. Instead, they operate within established structures for risk ownership, monitoring, reporting, business continuity, and management oversight.

SABIC’s framework classifies risks into compliance, financial, operational, and strategic categories and connects risk management with early warning, resilience, business continuity, and the protection of critical infrastructure. Its enterprise risk-management process is supported by integrated governance and informed by international risk and control practices (SABIC, 2024, pp. 43–45).

Saudi Aramco similarly applies an enterprise-wide framework covering strategic, operational, financial, and compliance risks. Its three-lines model assigns primary risk ownership to operating and support units, oversight and guidance to specialist risk functions, and independent assurance to internal audit (Saudi Aramco, 2024a, pp. 70–71). This structure is particularly relevant to an energy company operating complex assets under market, environmental, safety, regulatory, and technological uncertainty.

In the telecommunications case, stc’s disclosed framework connects risk management with strategic decision-making, management oversight, organizational controls, and cross-functional coordination. The framework addresses regulatory, sustainability, geopolitical, emerging-technology, cybersecurity, information-technology, and competitive risks (stc Group, 2024a, pp. 42–43).

These findings support the broader literature’s view that enterprise risk management creates value when it is incorporated into governance and strategic decision-making rather than treated as a separate compliance activity (Bakouche & Boughazi, 2022; Biresaw & Sibindi, 2025).

SABIC: Predictive Maintenance and Integrated Industrial Operations

The SABIC case shows that digital transformation is primarily directed toward industrial reliability, process integration, operational efficiency, safety, and data-supported decision-making. The company’s digital strategy emphasizes digitizing core processes, developing analytical and artificial-intelligence capabilities, strengthening data foundations, improving enterprise-resource planning, and developing employee digital skills (SABIC, 2024, pp. 91–92).

The STAR program represents a central element of this integration. As a next-generation enterprise platform, it is intended to connect people, devices, applications, and business networks while reducing fragmentation among operational systems. From a risk-management perspective, this integration may strengthen information consistency, process visibility, coordination, and the timely identification of operational problems (SABIC, 2024, p. 92).

The most direct link between digital transformation and risk management appears in asset monitoring. SABIC reports using artificial-intelligence-supported asset-care solutions to anticipate potential failures in critical equipment and facilitate earlier

maintenance. The company also uses robots, drones, and advanced inspection methods to assess tanks and flare systems, reducing the need for direct exposure to difficult inspection environments. Predictive tools combining raw-material quality, operational standards, and environmental conditions are further used to support production optimization and equipment performance (SABIC, 2024, p. 92).

These practices indicate that SABIC’s model links digital technologies primarily with operational risk, asset reliability, process safety, supply continuity, and industrial efficiency. The model supports the first analytical proposition because it emphasizes earlier detection and intervention. It also supports the second proposition because the selected applications correspond closely to the risk profile of a large petrochemical and manufacturing organization.

Saudi Aramco: Advanced Analytics for Complex Energy Risks

Saudi Aramco’s model emphasizes artificial intelligence, advanced computing, digital twins, blockchain, automation, and immersive technologies. These capabilities correspond to an operating environment characterized by complex physical assets, safety requirements, exploration uncertainty, production continuity, environmental exposure, and dependence on integrated information systems (Saudi Aramco, 2024a, pp. 70–71).

One significant application is i4Safety 2.0, an internally developed artificial-intelligence system that uses historical information to identify patterns associated with potential workplace risks. Its reported purpose is to support earlier risk recognition and strengthen operational safety. This illustrates a shift from recording incidents after their occurrence toward using accumulated information to support preventive decisions (Saudi Aramco, 2024b).

Advanced computing supports another category of risk. High-performance computing systems used in seismic imaging and reservoir simulation can process large volumes of technical information and improve the quality of subsurface interpretation. Such capabilities may reduce uncertainty in exploration and resource-development decisions, although the reviewed public documents do not provide sufficient evidence to quantify the resulting reduction in risk (Saudi Aramco, 2024b).

Digital-twin technology offers a further mechanism by creating continuously updated virtual representations of physical assets, systems, or processes. In principle, these models can support scenario analysis, condition monitoring, maintenance planning, and operational decision-making. Blockchain and smart contracts may strengthen transaction traceability and the execution of predefined contractual conditions, while automation can reduce variability and routine processing errors (Saudi Aramco, 2024b).

The Aramco case demonstrates that advanced technology is applied to technically complex and asset-intensive risks. Its integration model extends beyond process efficiency and emphasizes safety, exploration accuracy, asset integrity, continuity, and the management of large-scale operational uncertainty.

stc: Process Automation, Cloud Resilience, and Digital-Service Risk

The stc case reflects the risk environment of telecommunications and digital services. Compared with the two asset-intensive cases, greater attention is directed toward cybersecurity, information systems, regulatory exposure, emerging technologies, competition, service continuity, and process efficiency (stc Group, 2024a, pp. 42–43).

Robotic process automation is used to standardize repetitive administrative processes and reduce the likelihood of manual processing errors. Enterprise-resource-planning integration connects accounting, procurement, project monitoring, compliance, risk, and supply-chain functions, potentially improving information consistency and management visibility.

Cloud migration is also presented as a mechanism for improving flexibility, system efficiency, and continuity. The reported migration of a customer-experience management system to a cloud environment illustrates the use of scalable infrastructure to support service availability and organizational responsiveness (stc Group, 2024a). However, cloud adoption also introduces cybersecurity, third-party dependence, data-governance, and regulatory risks. Its risk-management value therefore depends on the strength of access controls, resilience planning, vendor oversight, and information-security governance.

The development of internal digital products and platforms may also reduce dependence on a single source of revenue and support service diversification. This connects digital transformation with strategic and competitive risk, not merely operational efficiency.

The stc case therefore supports the sector-alignment proposition. Its digital priorities reflect a service-based environment in which process speed, network and system availability, cybersecurity, scalability, and customer continuity are particularly important.

Cross-Case Comparison

The results can be summarized as follows:

Table 2. Cross-Sector Comparison of Digital Transformation Applications in Risk Management at SABIC, Saudi Aramco, and stc

Dimension	SABIC	Saudi Aramco	stc
Sector	Petrochemical and industrial	Energy	Telecommunications and digital services
Principal risk focus	Asset reliability, industrial operations, safety, supply continuity	Safety, asset integrity, exploration uncertainty, operational continuity	Cybersecurity, IT, service continuity, process reliability, competition
Main digital capabilities	AI, predictive maintenance, STAR platform, robots and drones	AI, advanced computing, digital twins, automation, blockchain	RPA, ERP integration, cloud services, digital platforms
Predominant risk function	Failure prediction and integrated operational control	Complex-risk modelling, safety	Process standardization, continuity, scalability, and control

		prediction, and asset monitoring	
Shared strategic direction	Proactive identification, earlier intervention, resilience, and data-supported decisions		

Source: Authors' compilation based on SABIC (2024), Saudi Aramco (2024a, 2024b), and stc Group (2024a, 2024b).

The strongest commonality is not the use of any single technology but the transition toward earlier risk recognition and intervention. All three organizations use digital capabilities to improve information availability, monitoring, anticipation, and decision support. This finding is consistent with the literature linking digital transformation with organizational responsiveness and sustainability (Afif & Khaloufi, 2022; Ben Said, 2022; Bourahla et al., 2023).

The principal difference concerns technology–risk alignment. SABIC prioritizes industrial reliability and predictive maintenance; Aramco emphasizes technically complex energy, safety, and asset risks; and stc concentrates more heavily on digital-service continuity, cybersecurity, cloud infrastructure, and process automation. The findings therefore support both study propositions.

Conditions for Effective Integration

The cross-case synthesis indicates that technological sophistication alone does not determine effective integration. Four enabling conditions recur across the cases.

First, digital initiatives require explicit alignment with material risks. A technology creates risk-management value when it addresses a clearly defined vulnerability rather than being adopted only because it is innovative.

Second, reliable and integrated data are essential. Artificial intelligence and predictive analytics depend on data completeness, consistency, relevance, and timeliness. Weak data foundations may produce unreliable predictions despite advanced technological infrastructure. This finding corresponds with Chaouchi and Khelouf's (2023) emphasis on data, human resources, technology, and processes as interdependent elements of digital transformation.

Third, governance and accountability remain necessary. Digital tools must be incorporated into risk ownership, escalation, monitoring, and decision-making arrangements. The enterprise frameworks reported by SABIC, Aramco, and stc indicate that technology is most useful when management responsibilities and control structures are clearly defined (SABIC, 2024; Saudi Aramco, 2024a; stc Group, 2024a).

Fourth, human capability remains important. Employees must be able to interpret digital outputs, challenge automated recommendations, and convert warnings into appropriate action. Digital transformation therefore complements rather than eliminates managerial and professional judgment.

Interpretation Boundaries

The findings demonstrate documented alignment between technologies and risk-management functions, but they do not establish causal effects. Public corporate reports describe initiatives, governance arrangements, and expected or reported benefits, yet they do not consistently provide comparable performance measures. The analysis therefore cannot determine whether one company's model is more effective than another or quantify reductions in incidents, financial losses, or operational disruption.

Moreover, stc-related source identification requires clarification. The materials appear to refer partly to solutions by stc and partly to stc Kuwait, while the article describes the case more broadly as stc Group. The final manuscript should identify the exact legal entity analyzed and use only its corresponding annual report and official disclosures.

Conclusion

This study examined how digital transformation is integrated with enterprise risk management in SABIC, Saudi Aramco, and stc. The comparative evidence indicates that the three organizations share a strategic movement away from predominantly reactive risk responses and toward continuous monitoring, earlier warning, predictive assessment, and proactive intervention. This finding supports the first study proposition and reinforces the view that digital transformation has become closely connected with organizational resilience and risk-informed decision-making.

The analysis also confirms that digital risk-management strategies are sector-dependent. SABIC applies artificial intelligence, integrated enterprise platforms, and advanced inspection technologies principally to industrial reliability, asset maintenance, safety, and operational coordination. Saudi Aramco employs artificial intelligence, advanced computing, digital twins, and related technologies to address complex safety, exploration, infrastructure, and energy-sector risks. stc places comparatively greater emphasis on automation, cloud infrastructure, enterprise systems, and digital platforms to strengthen process control, service continuity, cybersecurity, and competitive responsiveness. These differences support the second proposition that material risk exposure shapes technology selection.

The central theoretical conclusion is that integration should be evaluated through **technology–risk fit**, not through technological sophistication alone. An advanced system does not automatically strengthen risk management. Its value depends on whether it addresses a material vulnerability, uses reliable data, operates within an effective governance framework, and produces information that can be translated into timely organizational action.

The study also shows that digital transformation does not replace enterprise risk management. Instead, it changes the speed, scope, and analytical depth with which risk-management functions can be performed. Governance, accountability, human judgment, data quality, and business continuity remain essential. Digital tools generate the greatest value when embedded in these organizational capabilities.

From a managerial perspective, companies should begin with their most consequential vulnerabilities and select digital solutions that directly support the identification, assessment, monitoring, or mitigation of those risks. They should strengthen data governance, define accountability for algorithmic and automated decisions, develop employee analytical capabilities, and establish

measurable indicators linking digital initiatives with risk outcomes. Relevant indicators may include warning accuracy, equipment availability, incident frequency, process-error rates, service recovery time, forecast reliability, and continuity performance.

The study contributes a cross-sector analytical framework for understanding digital risk management in Saudi Arabia. Its findings are analytically informative but not statistically generalizable because the study examines only three cases and relies on public corporate disclosures. The absence of internal performance data and stakeholder interviews limits independent verification of organizational effectiveness. Future studies should adopt longitudinal designs, verify the exact stc entity under examination, incorporate interviews with risk and digital-transformation professionals, and test whether digital investments produce measurable improvements in resilience and risk performance.

Overall, the evidence suggests that the competitive and resilience benefits of digital transformation arise not from adopting the largest number of technologies, but from integrating appropriate technologies with specific risks, reliable data, capable personnel, and accountable governance.

Declarations

Ethics Approval: This study is based exclusively on publicly available corporate reports, governance disclosures, sustainability documents, and published scholarly sources. It did not involve human participants, animals, personal data, interviews, surveys, or experimental procedures. Therefore, ethics committee approval was not required.

Funding: The authors received no financial support for the research, authorship, or publication of this article.

Conflict of Interest: The authors declare that they have no financial, professional, institutional, or personal conflicts of interest that could have influenced the research or its conclusions. The authors have no commercial relationship with Saudi Aramco, SABIC, or stc.

Data Availability Statement: No original datasets were generated during this study. The evidence supporting the analysis was obtained from publicly available corporate reports, official company disclosures, and scholarly sources identified in the reference list. The structured information extracted from these documents may be obtained from the corresponding author upon reasonable request.

Author Contributions: Nabila Makhlouf contributed to the conceptualization, theoretical framework, methodology, comparative case-study design, and preparation of the original manuscript. Hanane Maalla contributed to data collection, document analysis, case-study development, and interpretation of the findings. Youssera Djehiche contributed to the cross-case comparison, validation of the analysis, preparation of recommendations, and critical revision of the manuscript. All authors reviewed and approved the final version and accept responsibility for the integrity and accuracy of the work.

Use of Generative Artificial Intelligence: Generative artificial intelligence tools were used for language refinement, translation assistance, and editorial organization. They were not used as primary data sources or as substitutes for documentary analysis and scholarly interpretation. The authors reviewed and verified the complete manuscript and assume full responsibility for its accuracy, originality, citations, analysis, and conclusions.

Ethical Approval

This study is based exclusively on the analysis of published texts, documentary and archival sources, and secondary literature. It does not involve human participants or animal subjects, and therefore ethics committee approval was not required. All sources are cited in accordance with academic integrity and copyright principles.

Acknowledgements

The authors thank the editors and the anonymous reviewers of the AJESS Journal for their constructive comments on an earlier version of this manuscript.

Declaration of Generative AI and AI-Assisted Technologies

The authors declare that no generative artificial intelligence (AI) or AI-assisted technologies were used in the design of the study, data collection, analyses, or interpretation of the scientific content of this manuscript. Any language-editing support was reviewed and verified by the authors, who take full responsibility for the content of the published article.

References

- Afif, H., & Khaloufi, W. (2022). The trend toward digital transformation: A necessity or a choice? *Economics, Finance, and Business Magazine*, 6(1).
- Bakouche, M., & Boughazi, F. (2022). The impact of risk management in achieving sustainable competitive advantage: A case study of the BECO Foundation project. *Journal of the Institute of Economic Sciences*, 25(1).
- Belkacem Elayachi, W. (2016). Risk management and future strategies: A case study of a mining company in Saudi Arabia. *Journal of Legal Studies*, 11(23).
- Ben Said, L. (2022). Trends of digital transformation in Algeria and their contributions to sustainable development. *Journal of Management and Economics Sciences*, 6(1).
- Biresaw, T., & Sibindi, A. (2025). A structured approach to enterprise risk management in Ethiopian commercial banks. *Risk Management Magazine*, 20(1).
- Bourahla, M., Saihi, K., & Elhamza, M. (2023). Digital transformation and its role in achieving the Sustainable Development Goals. *Journal of Environmental Studies and Sustainable Development*, 2(2).
- Bouzerouata, E., & Hammadi, M. (2024). Mechanisms of risk management in the economic institution. *Journal of Contemporary Economic Research*, 7(2).

- Chaouchi, K., & Khelouf, Z. (2023). Digital transformation in Algeria. *Accounting, Auditing, and Finance Magazine*, 5(1).
- Laroissi Graine, Z. (2021). The importance of risk management in small and medium-sized enterprises: A case study of the granite and concrete company SARL Agglolux in M'Sila. *El-Acil Journal for Economic and Administrative Research*, 5(2).
- SABIC. (2024). *Consolidated annual report 2024*. <https://www.sabic.com/ar/reports>
- Saudi Aramco. (2024a). *Annual report 2024: Risk*. <https://www.aramco.com/-/media/publications/corporate-reports/reports-and-presentations/2024/fy/sections/ara-2024-risk-arabic.pdf>
- Saudi Aramco. (2024b). *Digital technologies*. <https://www.aramco.com/ar/what-we-do/energy-innovation/digitalization/digital-technologies>
- stc Group. (2024a). *Annual report 2024*. <https://solutions.com.sa/wp-content/uploads/2021/09/solutions-by-stc.Annual-report-AR-pdf.pdf>
- stc Group. (2024b). *Enterprise risk management*. <https://cws.stc.com.kw/DigitalStatic/AnnualReport2024/Risk-Management-ar.html>

Genişletilmiş Özet

Giriş

Dijital dönüşüm, günümüzde kuruluşların rekabet gücünü, operasyonel sürekliliğini ve değişen çevresel koşullara uyum yeteneğini belirleyen temel stratejik unsurlardan biri hâline gelmiştir. Yapay zekâ, otomasyon, bulut bilişim, Nesnelerin İnterneti, ileri analitik ve gerçek zamanlı izleme sistemleri, yalnızca operasyonel verimliliği artırmak için değil, belirsizlikleri yönetmek ve daha isabetli kararlar almak için de kullanılmaktadır. Bu gelişmeler, geleneksel risk yönetimi anlayışının yeniden değerlendirilmesini gerekli kılmaktadır.

Geleneksel risk yönetimi çoğunlukla geçmiş verilere, dönemsel değerlendirmelere ve risk ortaya çıktıktan sonra uygulanan düzeltici önlemlere dayanmaktadır. Bununla birlikte teknolojik değişimin hızlanması, tedarik zincirlerinin karmaşıklaşması, siber tehditlerin artması ve kritik altyapıların birbirine bağımlı hâle gelmesi, yalnızca tepkisel yaklaşımların yetersiz kalmasına neden olmaktadır. Kuruluşlar bu nedenle sürekli izleme, erken uyarı, senaryo analizi ve öngörücü müdahale kapasitelerini geliştirmeye yönelmektedir.

Dijital teknolojilerin risk yönetimindeki değeri, yalnızca teknik gelişmişlik düzeyleriyle belirlenmemektedir. Kullanılan teknolojinin kuruluşun temel riskleriyle uyumu, veri kalitesi, yönetim yapısı, çalışanların dijital yeterlilikleri ve karar alma süreçleri de belirleyici olmaktadır. Ayrıca dijitalleşme, riskleri azaltırken siber güvenlik, veri gizliliği, sistem bağımlılığı ve algoritmik kararlar gibi yeni riskler de doğurabilmektedir.

Bu çalışma, dijital dönüşüm ile risk yönetimi arasındaki bütünleşmeyi Suudi Arabistan'daki üç büyük şirket üzerinden karşılaştırmalı olarak incelemektedir: enerji sektöründe Saudi Aramco, petrokimya ve sanayi sektöründe SABIC ve telekomünikasyon ile dijital hizmetler alanında stc. Araştırmanın temel amacı, şirketlerin ortak stratejik hedeflerini belirlemek ve sektörlere özgü risklerin teknoloji tercihlerine nasıl yansıdığını açıklamaktır. Çalışma, bütünleşmenin temel hedefinin tepkisel yönetimden proaktif ve öngörücü risk yönetimine geçiş olduğu; teknoloji seçimlerinin ise sektörlerin farklı risk profillerine göre şekillendiği önermelerinden hareket etmektedir.

Yöntem

Araştırmada nitel, betimleyici-analitik bir desen ile karşılaştırmalı çoklu durum çalışması yaklaşımı birlikte kullanılmıştır. Betimleyici-analitik bölümde dijital dönüşüm, kurumsal risk yönetimi, yapay zekâ, otomasyon, veri yönetimi ve örgütsel dayanıklılık arasındaki kavramsal ilişkiler açıklanmıştır. Uygulamalı bölümde ise Saudi Aramco, SABIC ve stc vakaları incelenerek farklı sektörlerde dijital teknolojiler ile risk yönetiminin nasıl bütünleştirildiği karşılaştırılmıştır.

Şirketler amaçlı ve maksimum çeşitlilik sağlayacak biçimde seçilmiştir. Seçimde şirketlerin Suudi ekonomisindeki stratejik önemleri, birbirinden farklı sektörlerde faaliyet göstermeleri, farklı risk profillerine sahip olmaları ve risk yönetimi ile dijital dönüşüme ilişkin kamuya açık kurumsal bilgiler sunmaları dikkate alınmıştır. Saudi Aramco enerji ve kritik fiziksel varlıklar; SABIC endüstriyel üretim, petrokimya ve tedarik zincirleri; stc ise telekomünikasyon, dijital hizmetler ve bilgi sistemleri bağlamında değerlendirilmiştir.

Araştırmanın temel zaman aralığı 2024 raporlama dönemidir. Veri kaynağı olarak şirketlerin yıllık veya bütünleşik raporları, risk yönetimi açıklamaları, sürdürülebilirlik belgeleri, yönetim bilgileri ve resmî dijital dönüşüm içerikleri kullanılmıştır. Akademik çalışmalar ise kurumsal çerçevenin oluşturulması ve kurumsal bulguların yorumlanması amacıyla değerlendirilmiştir.

Analiz birimi, "dijital risk yönetimi uygulaması" olarak belirlenmiştir. Bu kavram; dijital bir teknolojinin risklerin tanımlanması, değerlendirilmesi, öngörülmesi, izlenmesi, azaltılması veya raporlanmasına katkı sağlayan belgelenmiş kullanımını ifade etmektedir. Veriler; sektör bağlamı, risk profili, stratejik hedef, kullanılan teknoloji, risk yönetimi işlevi, yönetim yapısı, veri altyapısı, insan kaynağı ve bildirilen sonuçlar açısından kodlanmıştır.

Önce her şirket için ayrı bir vaka analizi yapılmış, ardından ortak bir karşılaştırma matrisi kullanılarak vakalar arası sentez gerçekleştirilmiştir. Bulgular benzerlikler, farklılıklar ve teknoloji-risk uyumu açısından değerlendirilmiştir. Şirket raporlarındaki açıklamalar doğrulanmış performans ölçümleri olarak değil, kurumsal uygulama ve stratejik yönelimlere ilişkin belge niteliğinde ele alınmıştır.

Bulgular ve Tartışma

Bulgular, üç şirketin de dijital teknolojileri daha erken risk tanımlama, sürekli izleme, öngörücü değerlendirme, operasyonel dayanıklılık ve veriye dayalı karar alma amaçlarıyla kullandığını göstermektedir. Bu ortak yönelim, riskler

gerçekleştikten sonra uygulanan düzeltici yaklaşımlardan, riskleri ortaya çıkmadan önce belirlemeyi ve etkilerini azaltmayı amaçlayan proaktif modellere geçişi ifade etmektedir.

SABIC'in dijital risk yönetimi modeli, sanayi ve petrokimya faaliyetlerinin gerektirdiği varlık güvenilirliği, süreç güvenliği, üretim sürekliliği ve operasyonel bütünlüşme üzerinde yoğunlaşmaktadır. Şirketin dijital stratejisi; temel süreçlerin dijitalleştirilmesini, yapay zekâ ve analitik yeteneklerin geliştirilmesini, veri altyapısının güçlendirilmesini ve çalışanların dijital yeterliliklerinin artırılmasını kapsamaktadır. STAR programı, insanlar, cihazlar ve işletme sistemleri arasındaki bilgi akışını bütünlüşterek parçalı sistemlerden kaynaklanan operasyonel riskleri azaltmayı hedeflemektedir. Yapay zekâ destekli varlık izleme çözümleri kritik ekipman arızalarını önceden tahmin etmeye, robotlar ve insansız hava araçları ise zorlu endüstriyel alanlarda denetim yapmaya yardımcı olmaktadır (SABIC, 2024, ss. 91–92).

Saudi Aramco'nun modeli, enerji sektörünün karmaşık fiziksel varlıkları, iş güvenliği, keşif belirsizliği, üretim sürekliliği ve çevresel riskleriyle uyumludur. Şirket yapay zekâ, yüksek performanslı hesaplama, dijital ikizler, otomasyon ve blokzincir gibi teknolojilerden yararlanmaktadır. i4Safety 2.0 sistemi, geçmiş verilerdeki örüntülerden hareketle potansiyel iş güvenliği risklerini belirlemeyi amaçlamaktadır. Gelişmiş hesaplama sistemleri sismik görüntüleme ve rezervuar modellemesini desteklerken dijital ikizler fiziksel varlıkların sanal modeller aracılığıyla izlenmesine ve farklı senaryoların değerlendirilmesine imkân sağlamaktadır (Saudi Aramco, 2024a, ss. 70–71; Saudi Aramco, 2024b).

stc vakasında ise siber güvenlik, bilgi teknolojileri, hizmet sürekliliği, rekabet, düzenleyici uyum ve gelişmekte olan teknolojiler ön plana çıkmaktadır. Robotik süreç otomasyonu, tekrarlayan işlemleri standartlaştırarak manuel hata riskini azaltmaktadır. Kurumsal kaynak planlama sistemlerinin bütünlüştirilmesi, farklı kurumsal fonksiyonlar arasında bilgi akışını geliştirmektedir. Bulut sistemlerine geçiş ise ölçeklenebilirlik, esneklik ve hizmet sürekliliğini desteklemektedir (stc Group, 2024a, ss. 42–43).

Karşılaştırmalı bulgular, teknoloji seçimlerinin sektörel riskler tarafından biçimlendirildiğini doğrulamaktadır. Bununla birlikte etkinlik yalnızca teknolojiye değil, güvenilir veriye, açık sorumluluklara, yönetim mekanizmalarına ve çalışanların analitik kapasitesine bağlıdır.

Sonuç ve Öneriler

Çalışma, dijital dönüşüm ile risk yönetiminin bütünlüştirilmesinin incelenen şirketlerde ortak bir stratejik yönelim oluşturduğu sonucuna ulaşmıştır. Saudi Aramco, SABIC ve stc farklı sektörlerde faaliyet göstermelerine rağmen riskleri daha erken belirlemek, sürekli izlemek, olası sonuçları tahmin etmek ve zamanında müdahale etmek amacıyla dijital kabiliyetlerden yararlanmaktadır. Bu sonuç, bütünlüşmenin temel hedefinin tepkisel risk yönetiminden proaktif ve öngörücü risk yönetimine geçiş olduğu yönündeki ilk araştırma önermesini desteklemektedir.

Bulgular, ikinci önermeyi de doğrulamaktadır. Şirketlerin teknoloji tercihleri, karşılaştıkları risklerin niteliğine göre farklılaşmaktadır. SABIC endüstriyel varlık güvenilirliği, üretim sürekliliği ve süreç güvenliği için yapay zekâ, gelişmiş denetim araçları ve bütünlüşik işletme platformlarına öncelik vermektedir. Saudi Aramco enerji altyapısı, güvenlik, keşif ve varlık bütünlüşü riskleri için yapay zekâ, ileri hesaplama ve dijital ikizlerden yararlanmaktadır. stc ise süreç otomasyonu, bulut altyapısı ve bütünlüşik bilgi sistemleri aracılığıyla siber güvenlik, hizmet sürekliliği ve operasyonel verimlilik risklerine odaklanmaktadır.

Çalışmanın temel kuramsal sonucu, dijital risk yönetiminin teknolojik gelişmişlikten çok “teknoloji–risk uyumu” üzerinden değerlendirilmesi gerektiğidir. Bir teknolojinin değeri, kuruluşun önemli bir riskine cevap vermesine, güvenilir verilerle çalışmasına, açık yönetim düzenlemelerine bağlanmasına ve karar alma süreçlerinde kullanılabilir çıktılar üretmesine bağlıdır.

Bu doğrultuda kuruluşların öncelikle en kritik kırılganlıklarını belirlemeleri ve dijital yatırımlarını bu risklere yönleltmeleri önerilmektedir. Veri doğruluğu, bütünlüşü, güvenliği ve erişilebilirliği güçlendirilmelidir. Otomatik ve algoritmik kararlar için sorumluluklar açıkça tanımlanmalı; çalışanların dijital ve analitik yeterlilikleri geliştirilmelidir. Dijital uygulamaların başarısı yalnızca kullanım oranlarıyla değil, erken uyarı doğruluğu, ekipman kullanılabilirliği, işlem hataları, hizmet iyileşme süresi, olay sıklığı ve iş sürekliliği gibi ölçülebilir risk göstergeleriyle değerlendirilmelidir.

Araştırma, kamuya açık kurumsal belgelere ve üç vakaya dayandığı için sonuçları istatistiksel olarak genellenemez. Gelecekteki araştırmalarda uzunlamasına tasarımlar, yönetici görüşmeleri, kurum içi performans göstergeleri ve dijital yatırım–risk performansı ilişkisini ölçen nicel yöntemler kullanılmalıdır. Ayrıca stc vakasında incelenen hukuki kuruluş açıkça belirlenmeli ve yalnızca ilgili kuruluşa ait resmî belgeler kullanılmalıdır.