RESEARCH ARTICLE

# Data Governance and Policy Support for Secure AI-Driven Corporate Digital Transformation

**Fang Sun** [1,*]

[1] Department of Business Administration, Dongshin University, Jeollanam-do 58245, Republic of Korea

## Abstract

**Artificial intelligence is becoming a core engine of corporate digital transformation, but its value depends first on secure, reliable, and accountable data and model infrastructures. As firms combine cloud platforms, edge devices, IoT sensors, digital twins, platform data, and algorithmic decision systems, they also expand the attack surface, privacy exposure, model security risk, and compliance burden. This paper develops a security-aware data and AI governance framework for AI-driven corporate digital transformation. It positions the framework as a unified governance model rather than a narrow extension of data management: data governance controls data classification, provenance, access, privacy, and sharing, while AI governance assures model validation, robustness, auditability, and accountability. The paper identifies six dilemmas: data sharing versus protection, weak provenance and pipeline security, adversarial or opaque AI models, vulnerabilities in cloud-edge-IoT and digital-twin ecosystems, unequal compliance capacity between large firms and SMEs, and fragmented coordination across cybersecurity, privacy, competition, and industrial policy. It then proposes an integrated agenda of tiered data governance, zero-trust and encryption-based security, privacy-enhancing collaboration, model validation and adversarial testing, algorithmic audit, incident response, regulatory sandboxes, certification, public secure data spaces, maturity indicators, and SME-oriented compliance services. The study contributes to reliable and secure computing research by showing that technical controls, organizational routines, and policy support must be integrated to enable trustworthy AI-driven transformation across firms of different sizes and sectors.**

**Keywords**: secure data governance, AI-driven corporate digital transformation, trustworthy AI, cybersecurity, privacy-preserving computation, compliance framework, model security.

## 1 Introduction

Corporate digital transformation has entered a new stage in which data and artificial intelligence jointly shape organizational processes, products, platforms, and business models [1, 2]. Earlier transformation programs mainly emphasized software deployment, enterprise information systems, online channels, and data analytics [3]. AI-driven transformation

**Submitted:** 10 May 2026
**Revised:** 30 June 2026
**Accepted:** 09 July 2026
**Published:** 21 July 2026

**Vol.** 2, **No.** 3, 2026.
10.62762/JRSC.2026.326448

***Corresponding author:**
✉ Fang Sun
sf2025@dsu.ac.kr

**Citation**
Sun, F. (2026). Data Governance and Policy Support for Secure AI-Driven Corporate Digital Transformation. *Journal of Reliable and Secure Computing*, 2(3), 164–178.

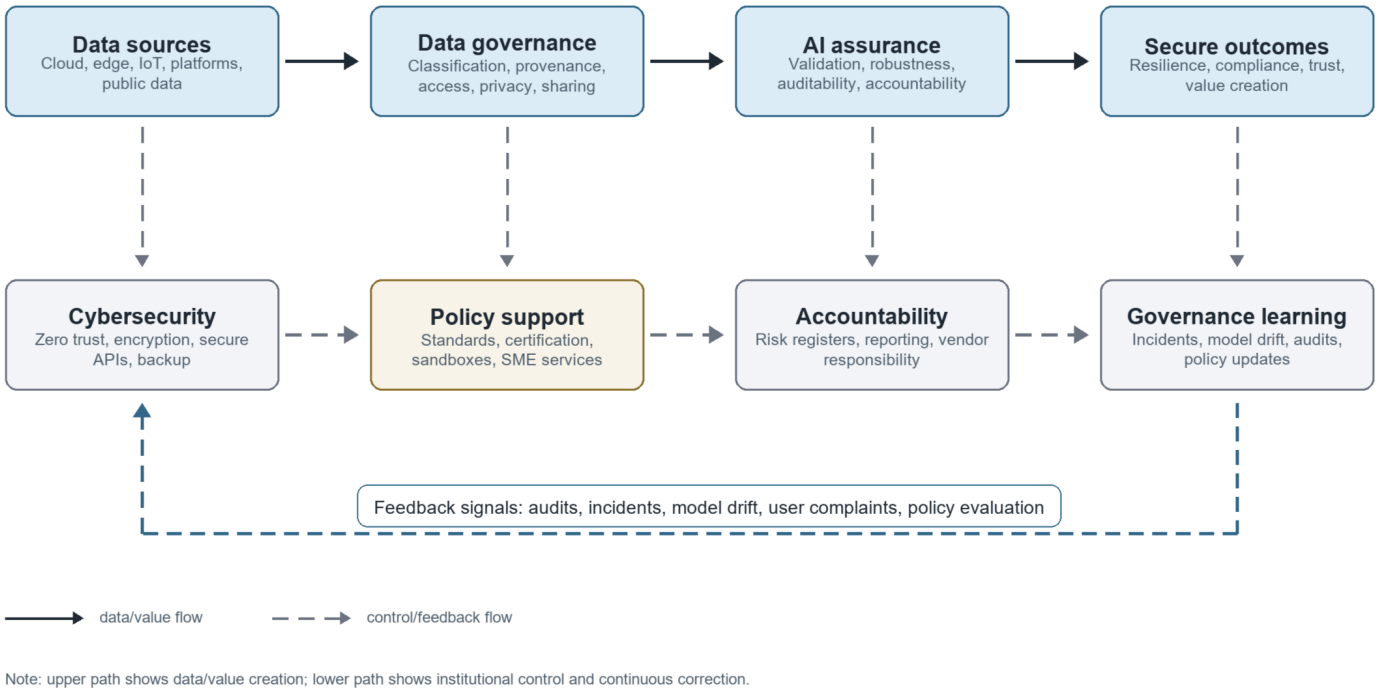


**Figure 1.** Security-aware data and AI governance framework for AI-driven corporate digital transformation.

goes further because algorithms convert data into predictions, classifications, recommendations, automated actions, and adaptive decision routines. This means that corporate transformation increasingly depends on whether data can be collected, shared, processed, protected, audited, and reused under conditions of security and trust.

The security dimension of this transformation has become central. Firms now build AI applications on cloud platforms, edge computing nodes, IoT devices, digital twins, application programming interfaces, and third-party data services. These technologies create operational efficiency and new forms of value creation, but they also generate cybersecurity, privacy, and system-resilience risks. Data pipelines may be manipulated, access controls may fail, models may be extracted or attacked, and automated decisions may create harm if data quality and accountability are weak. For this reason, data governance can no longer be treated as a back-office compliance task. It is part of secure and reliable computing infrastructure.

The issue is also a policy problem. Firms cannot independently create interoperable standards, trusted data spaces, certification systems, cross-sector accountability rules, or affordable compliance services for small and medium-sized enterprises. Public policy shapes the conditions under which data can circulate safely and under which AI systems can be used responsibly. Regulations such as the General Data Protection Regulation and the Data Governance Act illustrate a broad movement toward stronger privacy and data-access requirements [4, 5]. The Artificial Intelligence Act further strengthens risk management and AI accountability requirements [6]. At the same time, standards and risk-management frameworks such as the NIST AI Risk Management Framework and ISO/IEC 23894 are increasingly relevant to enterprise AI governance [7, 8]. Zero-trust architecture guidance is also important for secure enterprise data and AI environments [9].

This paper addresses the following question: how can data governance and policy support enable secure AI-driven corporate digital transformation while managing cybersecurity, privacy, reliability, and compliance risks? The question is intentionally interdisciplinary. It connects management research on digital transformation, information-systems research on data governance, cybersecurity research on secure architectures, and policy research on AI regulation and industrial support. The paper is designed as a conceptual and policy-oriented article rather than a narrow empirical study. Its goal is to develop a coherent framework and practical recommendations that are suitable for the security and reliability concerns of modern digital ecosystems.

The theoretical contribution is fourfold. First, the paper clarifies its conceptual positioning by treating the proposed framework as a unified data-and-AI

governance model: data governance provides upstream control over data assets and pipelines, while AI governance and assurance provide downstream control over model behavior, accountability, and resilience. Second, it extends data governance theory from decision rights and standards toward secure-computing capability, including provenance, zero-trust access, encryption, privacy-enhancing collaboration, and incident response [9]. Third, it complements AI governance frameworks such as the NIST AI RMF and ISO/IEC 23894 [7, 8] by specifying how enterprise data provenance, cybersecurity architecture, privacy-preserving computation, and policy support make risk management operational in organizational settings. Fourth, it advances trustworthy-AI and secure data lifecycle literature by linking enterprise controls with standards, certification, sandboxes, procurement rules, and SME-oriented implementation services.

The remainder of the paper is organized as follows. Section 2 introduces the conceptual background and presents a security-aware analytical framework. Section 3 analyzes the main security and regulatory dilemmas in AI-driven transformation. Section 4 develops a secure data and AI governance framework. Section 5 explains policy support mechanisms. Section 6 proposes an implementation roadmap and industrial best practices. Section 7 discusses theoretical, policy, and managerial implications. Section 8 concludes.

Figure 1 distinguishes data/value flow from control and feedback flow. Solid arrows indicate data/value flow, while dashed arrows indicate control and feedback flow. The upper horizontal path represents the data and value-creation flow: data sources are governed, transformed into AI-enabled outputs, assured, and converted into secure outcomes. The lower path represents the control and institutional flow: cybersecurity, policy support, accountability, and governance learning constrain and correct the value-creation process. The feedback loop is triggered by audits, incidents, model drift, user complaints, and policy evaluation. These signals update security controls, data-classification rules, assurance procedures, and policy instruments, thereby preventing governance from becoming static after deployment.

## 2 Conceptual Background and Research Positioning

This section clarifies the conceptual boundary of the paper. The proposed framework is primarily a unified governance model for both enterprise data and AI systems. It does not replace existing AI risk-management standards; rather, it explains how those standards can be embedded in enterprise data pipelines, cybersecurity architecture, privacy-preserving collaboration, and policy support. In this model, data governance is the upstream foundation that determines whether data are legitimate, traceable, protected, and reusable, whereas AI governance is the downstream assurance system that determines whether models are valid, robust, explainable where necessary, and auditable.

AI-driven corporate digital transformation refers to the redesign of business processes, decision systems, products, services, and ecosystem relationships through AI-enabled data processing. It differs from ordinary IT adoption because AI systems are data-intensive, probabilistic, and often embedded in continuous feedback loops. The same model may change its performance as data distributions shift, the same dataset may have different risk levels after combination, and the same algorithm may create different consequences depending on its deployment context. These characteristics create a need for continuous governance across both the data lifecycle and the AI model lifecycle [10]. How such governance should be designed—whether through centralised or distributed institutional arrangements—and how it applies across different organizational contexts, including public-sector deployments, are active questions in the emerging AI governance literature [11, 12]. These characteristics also extend governance requirements into the security and privacy domain: industrial IoT environments must be secured from the device level upward [14], data governance must be organized to support trustworthy AI across platforms and ecosystems [15], and privacy protection must be embedded into system design rather than added as an afterthought [13].

Data governance traditionally emphasizes decision rights, accountability, standards, and procedures for data assets [16–18]. In secure AI-driven transformation, this definition must be expanded. Data governance now encompasses a wide range of activities, including data inventories, classification, lineage, provenance, and consent management. It also covers technical controls such as access control, encryption, and privacy-enhancing computation, as well as organizational processes like model documentation, algorithmic audit, cybersecurity monitoring, vendor management, and incident

**Table 1.** Conceptual positioning of the proposed framework within reliable and secure computing research.

| Research area | Relevance to secure AI-driven transformation | Framework contribution |
|---|---|---|
| Reliable and fault-tolerant computing | AI transformation depends on stable data pipelines, fallback rules, redundancy, and recoverable digital services. | Introduces resilience controls, incident response, model-drift monitoring, fail-safe deployment, backup, and recovery mechanisms. |
| Formal verification and system resilience | High-impact AI systems require stronger assurance than ordinary software, especially where decisions affect rights, safety, or critical operations. | Discusses model validation, documentation, robustness testing, formal checks for critical components, and digital-twin-based pre-deployment testing. |
| Cybersecurity and privacy technologies | Data sharing, cloud services, APIs, and platform ecosystems increase exposure to data breaches and misuse. | Integrates zero-trust access control, encryption, data classification, privacy impact assessment, and privacy-preserving computation. |
| AI for security and security of AI | AI can detect threats, but AI systems can also be attacked through poisoning, evasion, extraction, and prompt-injection risks. | Analyzes adversarial AI risks and recommends red-team testing, model risk registers, monitoring, audit, and vendor accountability. |
| Secure architectures for cloud, edge, IoT, blockchain, and digital twins | Corporate data are increasingly generated and processed across distributed environments. | Develops a lifecycle architecture covering cloud-edge-IoT data pipelines, secure data spaces, blockchain traceability, and digital twins. |
| Compliance frameworks and industrial best practices | Firms need operational guidance to translate legal and ethical principles into auditable routines. | Provides policy support mechanisms, maturity stages, industrial best practices, and SME-oriented compliance services. |

response.

This distinction is important for theoretical positioning. Existing data governance studies usually focus on decision rights, stewardship, data quality, and organizational accountability. Existing AI governance frameworks usually focus on risk identification, model impact, transparency, human oversight, and lifecycle monitoring. The present framework advances both streams by showing that secure AI transformation requires a coupled governance logic: data controls shape the inputs, boundaries, and legitimacy of AI systems, while AI assurance controls shape the outputs, behavior, and accountability of automated decision systems.

Policy support refers to public or quasi-public mechanisms that make responsible transformation easier to implement. It includes fiscal incentives, infrastructure investment, secure data-sharing platforms, standards, procurement rules, certification, public data access, training, and regulatory experimentation. Policy support is not limited to promoting technology acquisition. It should also build the institutional conditions under which data can be used securely and under which AI systems can be audited and trusted.

This perspective contributes to reliable and secure computing research because corporate AI transformation now depends on secure architectures, privacy technologies, resilience, AI safety, and compliance frameworks. A firm adopting AI for supply-chain prediction, financial screening, industrial maintenance, or digital customer service must address confidentiality, integrity, availability, accountability, and recoverability. In this sense, the boundary between enterprise digital transformation and secure computing is increasingly porous.

Tables 1 and 2 summarize the conceptual positioning of the proposed framework relative to reliable and secure computing research and existing governance frameworks, respectively.

## 3 Security and Regulatory Dilemmas in AI-Driven Transformation

### 3.1 Data Sharing Versus Data Protection

AI systems normally improve when they can learn from large, diverse, and high-quality datasets. Firms

**Table 2.** Positioning of the proposed framework relative to existing governance frameworks.

| Existing framework or literature | Primary focus | Remaining gap for enterprise transformation | Added value of the proposed framework |
|---|---|---|---|
| NIST AI RMF and ISO/IEC 23894 [7, 8] | AI risk identification, measurement, management, and governance. | General AI risk guidance; limited detail on enterprise data pipelines, cloud-edge-IoT architecture, and SME support. | Embeds AI risk management in data provenance, cybersecurity architecture, privacy-enhancing collaboration, resilience, and implementation policy. |
| Zero-trust and cybersecurity guidance [9] | Identity-centric access control, network security, continuous verification, and incident response. | Protects systems, but does not fully cover model validity, algorithmic audit, data-sharing legitimacy, or AI accountability. | Connects zero-trust controls with AI assurance, lifecycle governance, vendor responsibility, and governance learning. |
| Secure data lifecycle literature [18, 33] | Data stewardship, classification, quality, privacy-enhancing computation, and secure data collaboration. | Protects datasets, but often underdevelops model behavior, adversarial testing, and downstream accountability. | Extends lifecycle governance into model training, deployment, monitoring, audit, and post-incident learning. |
| Trustworthy AI and algorithmic audit literature [27, 41] | Model documentation, transparency, fairness, accountability, and verifiable claims. | May overlook upstream data rights, provenance, secure architecture, and cross-firm implementation capacity. | Links trustworthy-AI tools to data governance, cyber resilience, procurement, certification, and SME support. |
| Proposed framework | Unified data-and-AI governance for secure corporate digital transformation. | Closes the gap between abstract AI principles and operational secure-computing practice. | Offers a five-layer model, lifecycle controls, maturity indicators, an illustrative scenario, and scalable policy support. |

therefore have strong incentives to combine internal operational data, customer data, supplier data, IoT data, and external public or platform data. However, wider data circulation increases privacy, cybersecurity, trade-secret, and unauthorized-inference risks. The dilemma is not simply whether data should be open or closed. The real issue is how to define usage rights, technical safeguards, purpose limitation, accountability, and revocation mechanisms for data that may be reused in multiple AI contexts [19–21].

This tension is especially visible in supply chains and platform ecosystems. A core enterprise may need supplier data for demand forecasting, quality control, and risk prediction. Suppliers may fear that data sharing will reveal business secrets or deepen dependency on dominant platforms. Consumers may benefit from personalized services while also facing profiling and discrimination risks. Secure governance must therefore enable data collaboration while preventing uncontrolled extraction and misuse.

### 3.2 Weak provenance and data pipeline security

AI transformation is only as reliable as the data pipeline behind it. If data sources are uncertain, timestamps are manipulated, interfaces are insecure, or data-cleaning steps are undocumented, model outputs become difficult to trust. Weak provenance also limits accountability after an incident. Firms may not know whether harm came from low-quality data, unauthorized access, vendor changes, model drift, or malicious manipulation.

Data pipeline risks are intensified by cloud migration, third-party APIs, edge computing, and IoT devices. Sensors may be compromised, edge nodes may have weak patching, and cloud storage may be misconfigured. Traditional perimeter security is insufficient because data move across organizational and technical boundaries. Secure transformation requires identity-based access, encryption, logging, data lineage, vulnerability management, and continuous monitoring across the full lifecycle.

### 3.3 Security of AI models

AI models create a distinct security challenge. Adversaries can attempt to poison training data, evade model detection, extract models through repeated queries, infer sensitive training information, or manipulate prompts in generative-AI workflows. These risks are no longer limited to specialized laboratories. Enterprise AI systems used for fraud detection, recruitment screening, predictive maintenance, document processing, and customer service may all be exposed to model security threats [22–24].

The problem is organizational as well as technical. Many firms adopt AI through vendors, cloud services, or open-source models. Downstream users may not control training data, model updates, parameter settings, or security testing. If contracts and documentation are weak, responsibility becomes diffuse. Firms may assume that vendors have ensured security, while vendors may assume that users will deploy systems responsibly. Secure data governance must therefore include model governance and vendor governance.

**Table 3.** Security and regulatory dilemmas in AI-driven corporate digital transformation.

| Dilemma | Typical manifestation | Security or reliability risk | Governance response |
|---|---|---|---|
| Data sharing versus protection | Firms need data collaboration across platforms, suppliers, customers, and public sources. | Privacy leakage, unauthorized inference, trade-secret exposure, and unclear usage rights. | Classified data governance, purpose limitation, contracts, consent, secure data spaces, and privacy-preserving computation. |
| Weak data provenance | Data sources, cleaning steps, interfaces, and lineage are poorly documented. | Unreliable models, manipulation, audit failure, and inability to attribute incidents. | Data lineage, metadata standards, logging, source verification, and provenance-based audit trails. |
| AI model security risks | Models may be poisoned, evaded, extracted, inverted, or manipulated through prompts. | Incorrect decisions, leakage of sensitive information, model theft, and safety failures. | Model risk registers, adversarial testing, red-team exercises, monitoring, and vendor documentation. |
| Distributed architecture risks | AI systems depend on cloud, edge, IoT, APIs, digital twins, and third-party services. | Expanded attack surface, cascading failures, insecure edge nodes, and misconfigured cloud assets. | Zero-trust architecture, encryption, segmentation, secure APIs, backup, redundancy, and recovery plans. |
| Opacity and assurance gaps | Model logic, data assumptions, and responsibility chains are unclear. | Low trust, weak accountability, discriminatory outcomes, and difficulty proving compliance. | Model cards, datasheets, impact assessment, explainability, formal checks for critical components, and algorithmic audit. |
| SME compliance gap | Small firms lack legal, technical, and organizational capacity. | Unsafe adoption, vendor lock-in, delayed transformation, and concentration of AI benefits. | Shared compliance services, templates, subsidized audits, training, and SME-oriented policy support. |

### 3.4 Distributed architecture and expanded attack surface

AI-driven transformation increasingly relies on distributed architectures. Cloud computing provides scalable storage and computation; edge computing supports low-latency processing; IoT devices generate industrial and operational data; blockchain may be used for traceability; and digital twins simulate physical systems. These architectures create new efficiencies but also expand the attack surface. A vulnerability in one layer can affect the entire transformation chain.

Digital twins and industrial AI systems illustrate the risk. A digital twin may integrate machine data, production schedules, maintenance records, and predictive models. If input data are compromised or simulation assumptions are not validated, operational decisions may become unsafe. In critical infrastructure and high-reliability environments, secure architecture must include redundancy, fail-safe rules, strict identity management, network segmentation, anomaly detection, and recovery procedures.

### 3.5 Opacity, accountability, and assurance gaps

Algorithmic opacity remains a major barrier to trustworthy transformation. Complex models may be difficult to interpret, and generative AI systems may produce outputs that are plausible but incorrect. When AI affects credit, employment, pricing, safety, or access to services, firms need evidence that models are valid, robust, fair, secure, and appropriately supervised. General ethical principles are not enough; firms need operational assurance tools [25–27]. These risks are closely related to the automation-augmentation paradox, black-box governance, algorithmic ethics, fairness, and AI safety frameworks [28–30].

Assurance gaps are also linked to formal verification and system resilience. Not every AI system can be fully verified in the same way as deterministic software, but high-impact components can be subject to structured validation, test coverage, constraint checking, adversarial evaluation, scenario testing, and audit trails. For critical use cases, digital twins and simulation environments can support pre-deployment testing before models are integrated into live operations.

### 3.6 SME compliance gaps and fragmented policy coordination

Large firms may have data-protection officers, cybersecurity teams, internal auditors, legal departments, and model risk specialists. SMEs often lack these resources. Yet SMEs must still adopt AI, cloud tools, digital marketing systems, and automated management software to remain competitive. If compliance requirements are complex and support is weak, SMEs may either avoid transformation or rely heavily on vendors without adequate oversight [31].

Regulatory fragmentation further increases the burden. AI-driven transformation cuts across cybersecurity, privacy, consumer protection, competition, labor, industrial policy, and sectoral regulation. Different agencies may issue overlapping guidance, while firms

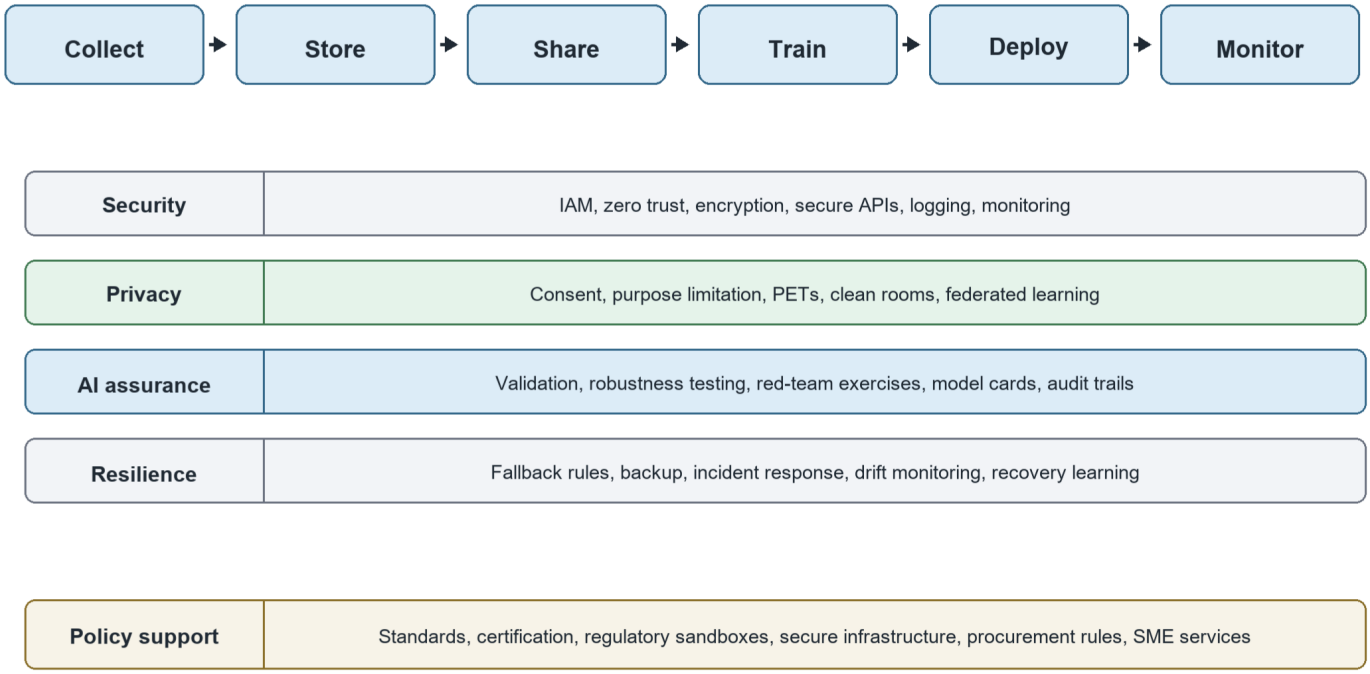


**Figure 2.** Secure data and AI lifecycle architecture.

struggle to identify which requirements apply. Policy coordination is therefore part of secure transformation. Without it, even well-intentioned firms may face uncertainty and delay investment.

The dilemmas discussed above are summarized in Table 3, which maps each dilemma to typical manifestations, security risks, and governance responses.

## 4 A Secure Data and AI Governance Framework

A security-aware framework should govern both data and models. Data governance without AI assurance may protect databases while leaving models vulnerable. AI governance without data governance may test models while ignoring the quality, legitimacy, and security of the data used to train or operate them. The proposed framework therefore combines five layers: data lifecycle governance, cybersecurity architecture, privacy-preserving data collaboration, AI assurance, and resilience management.

The first layer is data lifecycle governance. Firms should know what data they hold, where it came from, how it is classified, who can access it, how long it should be retained, and how it can be reused. This requires data inventories, data maps, metadata standards, lineage records, and approval procedures. Classification is especially important because personal information, industrial secrets, financial data, employee data, and safety-critical operational data require stronger controls than ordinary non-sensitive data.

The second layer is cybersecurity architecture. Secure transformation should be based on identity-centric access control rather than implicit trust in network location. Zero-trust principles require continuous verification of users, devices, applications, and data flows [9]. Encryption protects data at rest and in transit, while key management, backup, vulnerability scanning, secure APIs, and incident response protect the broader environment. Security must be embedded in the design of data pipelines rather than added after deployment.

The third layer is privacy-preserving data collaboration. Firms need data sharing for innovation, but direct data transfer is not always safe or lawful. Privacy-enhancing technologies can reduce this tension. Differential privacy can reduce re-identification risk in statistical outputs; federated learning can allow model training without centralizing raw data; secure multiparty computation and trusted execution environments can support joint computation under confidentiality constraints; and data clean rooms can provide controlled collaboration environments [32–34].

The fourth layer is AI assurance. Firms should maintain model documentation, data sheets, model cards, performance records, risk assessments, and audit trails for important AI systems [25–27]. Assurance should include data-quality checks, bias evaluation, robustness testing, adversarial testing, cybersecurity evaluation, explainability where appropriate, and human oversight. For generative AI, assurance should also address prompt injection, hallucination, data leakage, copyright and confidentiality concerns, and output monitoring.

The fifth layer is resilience management. AI systems can fail because of cyberattacks, model drift, data-distribution shifts, system outages, vendor failure, or unexpected user behavior. Firms should establish fallback procedures, recovery plans, redundancy, rollback mechanisms, incident escalation, and post-incident learning. Resilience is especially important when AI systems are embedded in production, logistics, energy management, finance, healthcare, or other high-impact operations.

Figure 2 presents the secure data and AI lifecycle architecture as a lifecycle flow supported by cross-cutting control layers. The top row is the data and model lifecycle flow, moving from collection and storage to sharing, training, deployment, and monitoring. The four horizontal bands are cross-cutting control flows: security controls protect identity, access, encryption, and infrastructure; privacy controls regulate lawful and privacy-preserving collaboration; AI assurance controls validate model performance, robustness, and auditability; and resilience controls ensure fallback, backup, incident response, and recovery. Policy support provides external enabling conditions through standards, certification, regulatory sandboxes, procurement rules, secure infrastructure, and SME services. Figure 2 illustrates the secure data and AI lifecycle architecture, while Table 4 provides detailed governance controls across each lifecycle stage.

## 5 Policy Support Mechanisms for Secure Transformation

Policy support should make secure AI transformation easier, not merely make AI adoption cheaper. A subsidy that helps firms purchase AI software may increase transformation statistics, but it does not necessarily improve data quality, privacy protection, cybersecurity maturity, or model accountability. Public support should therefore be tied to governance milestones and security capabilities. The goal is not to slow innovation; it is to reduce the probability that innovation creates avoidable harm.

The first mechanism is standards and certification. Firms need practical guidance that translates broad legal and ethical principles into operational controls. Standards for information security, AI risk management, privacy impact assessment, model documentation, and cloud security reduce uncertainty. Certification can help markets distinguish trustworthy providers from vendors that shift risk to users. For high-impact systems, certification should be risk-based and proportionate rather than uniform across all applications.

The second mechanism is secure digital infrastructure. AI transformation depends on shared infrastructure such as cloud computing, edge networks, industrial internet platforms, public data portals, cybersecurity monitoring systems, and secure data spaces. Public investment can lower shared costs, especially for SMEs and traditional industries. Infrastructure should include technical safeguards and institutional rules, including metadata standards, access controls, dispute-resolution procedures, and accountability requirements.

The third mechanism is regulatory experimentation. AI applications change quickly, and fixed rules may become outdated. Regulatory sandboxes and pilot zones allow firms to test novel applications under supervision while regulators learn about risks. Sandboxes are useful for emerging areas such as AI-based financial risk assessment, healthcare decision support, industrial digital twins, energy optimization, and automated supply-chain coordination. They should include security testing, privacy review, documentation, and post-pilot evaluation.

The fourth mechanism is SME-oriented compliance support. Secure AI governance contains fixed costs that small firms cannot easily absorb. Governments, universities, chambers of commerce, and industry associations can establish data-governance service centers that provide templates, training, legal guidance, cybersecurity testing, model risk checklists, and low-cost audits. This prevents responsible AI from becoming a capability available only to large firms.

Scalability is particularly important for developing countries and SMEs. In resource-constrained settings, the framework should be adopted progressively rather than as a one-step compliance package. A

**Table 4.** Governance controls across the secure data and AI lifecycle.

| Lifecycle stage | Main risks | Enterprise controls | Policy support |
|---|---|---|---|
| Data collection | Unlawful collection, weak consent, unverified sources, IoT manipulation. | Source verification, consent records, logging, data minimization, secure sensor configuration. | Sectoral guidance, consent templates, security baselines for IoT and industrial devices. |
| Data storage | Misclassification, unauthorized access, misconfigured cloud storage, leakage. | Data classification, encryption, key management, access control, backup, retention rules. | Cloud security standards, certification, shared secure infrastructure, audit requirements. |
| Data sharing | Re-identification, trade-secret exposure, insecure APIs, unclear responsibilities. | Standard contracts, secure APIs, data spaces, federated learning, clean rooms, differential privacy. | Trusted data intermediaries, legal recognition of data-sharing mechanisms, public data spaces. |
| Model training | Data poisoning, bias, low data quality, undocumented assumptions. | Provenance checks, data sheets, bias testing, robust training, access controls for training data. | Model risk guidance, benchmarking datasets, sandbox testing, training subsidies. |
| Model deployment | Adversarial attacks, model extraction, unsafe automation, lack of oversight. | Red-team testing, rate limits, monitoring, human oversight, fail-safe rules, vendor controls. | Certification for high-risk AI, procurement rules, incident reporting mechanisms. |
| Monitoring and audit | Model drift, hidden failures, compliance gaps, accountability disputes. | Audit trails, model cards, drift monitoring, incident response, independent audit. | Auditor qualification, reporting templates, regulatory feedback loops, SME audit support. |

**Table 5.** Policy support mechanisms for secure AI-driven corporate transformation.

| Policy area | Concrete instrument | Target group | Expected effect |
|---|---|---|---|
| Standards and certification | AI risk management standards, information-security baselines, audit templates, certification for high-risk systems. | All firms and AI vendors. | Translate abstract principles into verifiable controls and increase market trust. |
| Secure infrastructure | Public secure data spaces, industrial internet platforms, cloud security support, edge and IoT baselines. | Regional clusters, supply chains, SMEs, and critical sectors. | Lower shared costs, improve interoperability, and reduce security gaps. |
| Fiscal incentives | Tax deductions, vouchers, grants, and loans tied to data security, privacy, and model-assurance milestones. | SMEs and traditional firms. | Encourage durable governance capability rather than superficial AI procurement. |
| Regulatory sandboxes | Supervised pilots with privacy review, security testing, model documentation, and feedback reports. | Innovative firms in uncertain or high-impact sectors. | Balance experimentation with risk monitoring and policy learning. |
| SME service centers | Templates, legal support, training, cybersecurity testing, low-cost audits, model risk checklists. | SMEs and start-ups. | Reduce fixed compliance costs and prevent unsafe vendor dependency. |
| Procurement and vendor rules | Security and auditability requirements for public digital procurement; standard AI vendor clauses. | Cloud, AI, platform, and software providers. | Create market incentives for secure and trustworthy AI products. |
| Coordination and interoperability | Interagency portals, joint guidance, compatible certification, international standards participation. | Firms facing overlapping rules or cross-border data flows. | Reduce regulatory uncertainty and improve compliance efficiency. |

realistic pathway begins with low-cost data inventories, basic access control, backup, staff training, vendor checklists, and shared audit templates. More advanced tools, such as secure data spaces, federated learning, independent model audit, and certification, can then be introduced through sectoral service centers, public cloud-security support, university-industry laboratories, and regional digital-transformation programs. This phased approach prevents secure AI governance from becoming an exclusive capability of large firms and advanced economies.

The fifth mechanism is public procurement and vendor accountability. Governments are major buyers of digital services, and procurement rules can shape market behavior. Procurement should require suppliers to demonstrate cybersecurity, privacy protection, interoperability, auditability, incident response, and data portability. Vendor contracts should include documentation obligations, security-assurance commitments, data-processing information, and support for regulatory compliance. These requirements are important because many firms rely on external AI vendors.

The sixth mechanism is international and cross-sector interoperability. Firms operating in global markets face different privacy, cybersecurity, data-transfer, and AI-risk rules. Full harmonization is unrealistic, but interoperability can reduce unnecessary friction.

Governments can align terminology, participate in standards, provide guidance for cross-border transfers, and recognize compatible certification systems while preserving legitimate public interests. This interoperability agenda is consistent with international AI ethics principles, OECD AI guidance, and whole-of-government digital policy frameworks [35–37].

Table 5 summarizes the policy support mechanisms discussed in this section, along with their target groups and expected effects.

## 6 Implementation Roadmap and Industrial Best Practices

### 6.1 Illustrative manufacturing scenario

Consider a medium-sized manufacturing firm that deploys an AI-based predictive-maintenance system connected to industrial IoT sensors and a production-line digital twin. The data flow begins with machine vibration, temperature, energy-use, maintenance, and quality-inspection data. These data are stored in a cloud-edge architecture and used to train models that predict equipment failure and recommend maintenance schedules. The business benefit is reduced downtime and better production planning, but the system also creates security and accountability risks: sensor data may be manipulated, cloud storage may be misconfigured, vendors may update models without adequate documentation, and false predictions may interrupt production.

The proposed framework operationalizes governance in this scenario. Data lifecycle governance requires source verification, lineage records, classification of sensitive production data, and access matrices for engineers, suppliers, and vendors. Cybersecurity architecture applies identity-based access, encryption, secure APIs, network segmentation, backup tests, and incident-response rules. Privacy-preserving collaboration allows the firm to share selected maintenance patterns with equipment suppliers through clean rooms or federated learning rather than transferring raw production data. AI assurance requires model cards, validation reports, red-team testing, drift monitoring, human override, and audit trails. Resilience management requires fallback maintenance rules and post-incident learning when a model error or cyber event occurs. Policy support can reduce adoption costs through sectoral templates, subsidized security testing, certification guidance, and SME-oriented service centers.

### 6.2 Roadmap and maturity operationalization

A practical roadmap should proceed from diagnosis to continuous improvement. The first stage is capability diagnosis. Firms should assess data inventories, cybersecurity maturity, privacy procedures, cloud configuration, AI use cases, vendor dependencies, incident response, and existing compliance responsibilities. Policy makers should also diagnose sector-level maturity rather than assume that all firms begin from the same baseline.

The second stage is data classification and governance design. Firms should classify data according to sensitivity, identifiability, business value, security relevance, and potential harm. Data classification should be linked to access rights, encryption, retention, sharing rules, and audit obligations. This stage creates the foundation for proportional governance: low-risk data should not be overregulated, but high-risk data should receive strong controls.

The third stage is security hardening. Firms should implement identity and access management, multi-factor authentication, least-privilege access, encryption, secure APIs, vulnerability management, cloud-configuration review, endpoint security, backup, and disaster recovery. For distributed AI environments, security hardening should cover edge devices, IoT sensors, data connectors, model-serving infrastructure, and third-party platforms.

The fourth stage is AI assurance. Firms should maintain an AI inventory, model risk register, model cards, data sheets, validation reports, human-oversight procedures, and incident-response rules. High-impact systems should undergo adversarial testing, fairness review, robustness checks, explainability assessment, and independent audit where appropriate. Generative AI applications require additional controls for prompt injection, confidential data leakage, hallucination, and output accountability.

The fifth stage is trusted collaboration. After internal controls are established, firms can participate in secure data spaces, supply-chain data sharing, federated learning, clean rooms, or blockchain-based traceability. Collaboration should be based on standard contracts and technical safeguards. SMEs may benefit from collective data infrastructures because they often lack sufficient data to develop advanced AI systems independently.

The sixth stage is continuous monitoring and policy learning. Security and AI risks evolve. Firms

**Table 6.** Implementation roadmap and industrial best practices.

| Stage | Enterprise action | Best-practice indicator | Policy enabler |
|---|---|---|---|
| 1. Diagnose capability | Map AI use cases, data assets, cloud dependencies, vendors, and compliance obligations. | AI inventory, data inventory, maturity assessment, risk register. | Sectoral maturity assessment and public self-assessment tools. |
| 2. Classify data | Classify data by sensitivity, identifiability, security relevance, and potential harm. | Classification policy, access matrix, retention schedule, approval workflow. | Sector-specific classification guidance and templates. |
| 3. Harden architecture | Adopt zero-trust principles, encryption, secure APIs, backup, endpoint security, and vulnerability management. | Access logs, cloud security review, patching evidence, backup tests, incident plan. | Security baselines, certification, cloud-security support, shared monitoring. |
| 4. Assure AI models | Validate models, document data and assumptions, test robustness, and define human oversight. | Model cards, datasheets, validation report, red-team results, audit trail. | AI assurance standards, auditor ecosystem, sandbox testing. |
| 5. Collaborate safely | Use data spaces, federated learning, clean rooms, and standard contracts for data sharing. | Signed data-sharing agreement, privacy-enhancing computation, provenance record. | Trusted intermediaries, standard clauses, public secure data platforms. |
| 6. Monitor and improve | Track incidents, model drift, complaints, vendor updates, and compliance costs. | Incident metrics, drift alerts, audit schedule, post-incident review. | Policy evaluation, reporting templates, guidance updates, SME service centers. |

should monitor model drift, security incidents, access anomalies, privacy complaints, audit findings, and vendor changes. Regulators should use evidence from sandboxes, incident reports, compliance costs, and SME participation to update guidance and support mechanisms. Continuous learning prevents governance from becoming outdated.

For implementation, maturity can be measured across the five layers of the framework. The aim is not to create a rigid universal score, but to help firms identify whether they have only basic documentation, operational controls, or continuous assurance and learning. Table 6 presents the six-stage implementation roadmap with corresponding enterprise actions, best-practice indicators, and policy enablers, while Table 7 provides an illustrative maturity structure across the five governance layers that can be adapted by sector and firm size.

## 7 Discussion

The analysis has several theoretical implications. First, it suggests that AI-driven corporate digital transformation should be studied as a security-aware data governance process. Digital transformation theories often emphasize strategy, technology adoption, and organizational change [1], while information systems research highlights that technology adoption alone does not guarantee value creation, since the benefits of connected technologies such as IoT are systematically offset by governance, security, and risk management challenges that require complementary organizational capabilities [38]. These perspectives remain important, but they are incomplete without secure computing. AI transformation cannot create sustainable value if data pipelines are insecure, models are vulnerable, and accountability is weak. It also reflects the productivity-paradox and analytics-capability literature, which suggests that digital value depends on complementary organizational and governance capabilities rather than technology adoption alone [39, 40].

Second, the paper connects reliable and secure computing to public policy. Secure AI transformation is not produced only by enterprise controls or only by regulation. It requires a combination of technical mechanisms, organizational routines, and enabling institutions. Standards, certification, sandboxes, secure infrastructure, vendor accountability, and SME service centers are not external to computing practice; they shape whether secure computing can be implemented across heterogeneous firms. This view is also consistent with trustworthy-AI development work that emphasizes verifiable claims, evidence, and accountable assurance mechanisms [41].

Third, the paper highlights the importance of proportionality and scalability. A small enterprise using AI for inventory forecasting should not face the same governance burden as a bank using AI for credit scoring or a hospital using AI for clinical triage. At the same time, every AI adopter needs basic safeguards for data security, privacy, and accountability. Proportional

**Table 7.** Maturity indicators across the five-layer governance model.

| Governance layer | Basic maturity evidence | Advanced maturity evidence | Possible KPIs |
|---|---|---|---|
| Data lifecycle governance | Data inventory, classification policy, ownership map, retention rules, access matrix. | Automated lineage, provenance-based audit, data-quality dashboards, continuous policy review. | Classification coverage; lineage coverage; datasets with owners; access-review completion rate. |
| Cybersecurity architecture | Multi-factor authentication, least-privilege access, encryption, backup, incident plan. | Zero-trust segmentation, continuous monitoring, tested recovery, supplier security assurance. | Encryption coverage; patch latency; incident-response time; backup-test success rate. |
| Privacy-preserving collaboration | Consent records, purpose limitation, data-sharing contracts, privacy impact review. | Federated learning, clean rooms, differential privacy, secure multiparty computation for sensitive collaboration. | Collaborations using PETs; privacy-impact assessments completed; re-identification incidents. |
| AI assurance | AI inventory, model documentation, validation report, human oversight, vendor documentation. | Adversarial testing, red-team review, independent audit, drift monitoring, model cards and datasheets. | Models with validation reports; testing frequency; drift-alert closure time; audit coverage. |
| Resilience and governance learning | Fallback rules, escalation procedure, incident log, post-incident review. | Scenario testing, digital-twin simulation, board-level reporting, policy-learning feedback loop. | Mean time to recover; post-incident actions closed; resilience-test frequency; governance-review cycle. |

governance helps avoid both underprotection and excessive compliance costs. For developing countries, local governments, and SMEs, the most feasible approach is a staged model: establish baseline controls first, then scale toward certification, secure data spaces, independent audit, and advanced AI assurance as infrastructure and organizational capacity improve.

The managerial implications are direct. Managers should treat data governance as part of corporate strategy and cybersecurity governance. AI adoption should begin with questions about data quality, data rights, access control, vendor responsibility, model validation, human oversight, and recovery plans. A purchase-based view of AI transformation is risky because software acquisition does not automatically create secure or reliable capabilities.

Boards and senior executives should also establish clear accountability for data and AI. Responsibility should not be fragmented among IT departments, legal teams, vendors, and business units. Firms need cross-functional governance committees, escalation procedures, internal audit, privacy and security roles, and employee training. Employees should understand how to use AI systems responsibly, how to report errors, and when human judgment should override automated outputs.

For technology vendors and platform firms, the paper implies heightened responsibility. Vendors influence the security and compliance capacity of many downstream users, especially SMEs. They should provide documentation, model limitations, security assurances, update notices, data-processing information, and support for audit. If vendors design opaque systems or restrict data portability, they weaken the broader digital transformation ecosystem. These concerns also relate to ecosystem governance and the risk that data concentration can reinforce asymmetric market power in the digital economy [42, 43].

The paper has limitations. It develops a conceptual and policy framework rather than testing causal effects. Future empirical research could measure whether secure data-governance maturity improves the relationship between AI adoption and firm performance, whether SME service centers reduce compliance costs, or whether regulatory sandboxes improve responsible innovation. Sector-specific studies could examine finance, manufacturing, healthcare, logistics, energy, retail, and platform ecosystems.

Future research should also develop better metrics for secure data-governance capability. Possible indicators include data inventories, classification coverage, access-control maturity, encryption coverage, privacy-impact assessments, model documentation, adversarial testing frequency, audit adoption, incident-response time, and participation in secure data spaces. Better measurement would strengthen policy evaluation and allow researchers to distinguish superficial AI adoption from secure transformation.

## 8 Conclusion

AI-driven corporate digital transformation depends on data, but data create value only when they can be used

securely, responsibly, and reliably. As firms integrate cloud computing, edge devices, IoT systems, digital twins, platforms, and AI models, the boundaries between digital transformation, cybersecurity, privacy, model assurance, and compliance become increasingly blurred. This paper therefore positioned data governance and AI governance as coupled components of a unified secure-computing capability rather than as separate managerial or ethical functions.

This paper developed a security-aware framework linking data lifecycle governance, cybersecurity architecture, privacy-preserving collaboration, AI assurance, resilience management, and policy support. It identified six major dilemmas: data sharing versus data protection, weak provenance and pipeline security, AI model security risks, distributed-architecture vulnerabilities, opacity and assurance gaps, and unequal compliance capacity. These dilemmas show why technology adoption alone cannot produce trustworthy transformation.

The paper proposed policy support mechanisms including standards, certification, secure infrastructure, fiscal incentives tied to governance milestones, sandboxes, SME service centers, procurement rules, vendor accountability, and interoperability mechanisms. It also proposed an implementation roadmap from diagnosis and data classification to architecture hardening, AI assurance, trusted collaboration, and continuous monitoring.

For policy makers, the central message is that secure data governance should be treated as productive infrastructure. For firms, the central message is that AI transformation requires governance capability, not only technical tools. For researchers, the central message is that future studies of corporate digital transformation should integrate cybersecurity, privacy technologies, AI assurance, system resilience, and policy design. High-quality AI-driven transformation will depend on whether societies can make data useful, secure, accountable, and fairly accessible.

## Data Availability Statement

Data will be made available on request.

## Funding

This work was supported without any funding.

## Conflicts of Interest

The author declares no conflicts of interest.

## AI Use Statement

The author declares that no generative AI was used in the preparation of this manuscript.

## Ethical Approval and Consent to Participate

Not applicable.

## References

[1] Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of business research, 122*, 889-901. [CrossRef]

[2] Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. V. (2013). Digital business strategy: toward a next generation of insights. *MIS quarterly, 37*(2), 471-482. [CrossRef]

[3] Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2013). Embracing digital technology: A new strategic imperative. *MIT sloan management review, 55*(2), 1. https://sloanreview.mit.edu/projects/scholars/embracing-digital-technology/

[4] European Parliament and Council. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[5] European Parliament and Council. (2022). Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). *Official Journal of the European Union*. http://data.europa.eu/eli/reg/2022/868/oj

[6] European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. http://data.europa.eu/eli/reg/2024/1689/oj

[7] Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). *National Institute of Standards and Technology*. [CrossRef]

[8] ISO/IEC. (2023). ISO/IEC 23894:2023 Information technology - Artificial intelligence - Guidance on risk management. *International Organization for Standardization*. https://www.iso.org/standard/77304.html

[9] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (No. NIST Special Publication (SP) 800-207). National Institute of Standards and Technology. [CrossRef]

[10] Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics, 2*(4), 603-609. [CrossRef]

[11] Cihon, P., Maas, M. M., & Kemp, L. (2020,

February). Should artificial intelligence governance be centralised? Design lessons from history. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (pp. 228-234). [CrossRef]

[12] Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector—applications and challenges. *International journal of public administration, 42*(7), 596-615. [CrossRef]

[13] Rubinstein, I. S. (2011). Regulating privacy by design. *Berkeley Tech. LJ, 26*, 1409.

[14] Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in industry, 101*, 1-12. [CrossRef]

[15] Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government information quarterly, 37*(3), 101493. [CrossRef]

[16] Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM, 53*(1), 148-152. [CrossRef]

[17] Weber, K., Otto, B., & Österle, H. (2009). One size does not fit all—a contingency approach to data governance. *Journal of Data and Information Quality (JDIQ), 1*(1), 1-27. [CrossRef]

[18] Abraham, R., Schneider, J., & Vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International journal of information management, 49*, 424-438. [CrossRef]

[19] OECD. (2022). Going Digital to Advance Data Governance for Growth and Well-being. *OECD Publishing*. [CrossRef]

[20] Tene, O., & Polonetsky, J. (2011). Privacy in the age of big data: a time for big decisions. *Stan. L. Rev. Online, 64*, 63.

[21] Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2021). Data analytics in a privacy-concerned world. *Journal of Business Research, 122*, 915-925. [CrossRef]

[22] Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*. [CrossRef]

[23] Papernot, N., McDaniel, P., Sinha, A., & Wellman, M. P. (2018, April). Sok: Security and privacy in machine learning. In *2018 IEEE European symposium on security and privacy (EuroS&P)* (pp. 399-414). IEEE. [CrossRef]

[24] Biggio, B., & Roli, F. (2018, October). Wild patterns: Ten years after the rise of adversarial machine learning. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security* (pp. 2154-2156). [CrossRef]

[25] Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., ... & Gebru, T. (2019, January). Model cards for model reporting. In *Proceedings of the conference on fairness, accountability, and transparency* (pp. 220-229). [CrossRef]

[26] Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Iii, H. D., & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM, 64*(12), 86-92. [CrossRef]

[27] Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., ... & Barnes, P. (2020, January). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 conference on fairness, accountability, and transparency* (pp. 33-44). [CrossRef]

[28] Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation–augmentation paradox. *Academy of management review, 46*(1), 192-210. [CrossRef]

[29] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big data & society, 3*(2), 2053951716679679. [CrossRef]

[30] Leslie, D. (2019). Understanding Artificial Intelligence Ethics and Safety: A Guide for the Responsible Design and Implementation of AI Systems in the Public Sector. *The Alan Turing Institute*. [CrossRef]

[31] Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., ... & Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International journal of information management, 57*, 101994. [CrossRef]

[32] Dwork, C. (2008, April). Differential privacy: A survey of results. In *International conference on theory and applications of models of computation* (pp. 1-19). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[33] Kairouz, P., & McMahan, H. B. (2021). Advances and open problems in federated learning. *Foundations and trends in machine learning, 14*(1-2), 1-210. [CrossRef]

[34] Lindell, Y. (2020). Secure multiparty computation. *Communications of the ACM, 64*(1), 86-96. [CrossRef]

[35] UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. *United Nations Educational, Scientific and Cultural Organization*. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence

[36] OECD. (2024). Recommendation of the Council on Artificial Intelligence. *OECD Legal Instruments*. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

[37] OECD. (2020). Going Digital integrated policy framework. *OECD Digital Economy Papers, No. 292*. OECD Publishing. [CrossRef]

[38] Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management, 51*, 101952. [CrossRef]

[39] Brynjolfsson, E., Rock, D., & Syverson, C. (2018). Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics. In *The economics of artificial intelligence: An agenda* (pp. 23-57). University of Chicago Press. https://www.nber.org/system/files/chapters/c14007/c14007.pdf

[40] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and machines, 28*(4), 689-707. [CrossRef]

[41] Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., ... & Anderljung, M. (2020). Toward trustworthy AI development: mechanisms for supporting verifiable claims. *arXiv preprint arXiv:2004.07213*. [CrossRef]

[42] Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. *Journal of management, 43*(1), 39-58. [CrossRef]

[43] Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs. https://www.hbs.edu/faculty/Pages/item.aspx?num=56791