Registered in Germany Europa Revue Journal
ISSN: 1862-6564 Vol. 6 No. 9 (2026) Published September 30, 2026

THE ROLE OF BIG DATA ANALYTICS IN IMPROVING ENTERPRISE DECISION-MAKING

Samir Bakhtiyarov

Azerbaijan State University of Economics (UNEC) *BSc in Information Technology; MBA in Risk Management and Engineering*

Abstract

Enterprises generate data through transactions, customer interactions, sensors, websites, mobile applications and internal information systems. The managerial value of this data depends not on its volume alone but on whether it can be converted into timely, reliable and relevant information for decisions.

Keywords

big data, business analytics, decision-making, data governance, predictive analytics, information technology, risk management, enterprise systems.

Introduction

NIST describes big data in the context of a networked, digitized and sensor-rich environment in which the volume, velocity and variety of data can exceed traditional technical approaches. This creates both an opportunity and a management problem: organizations can observe operations in greater detail, but poor architecture and weak governance can make the same data difficult to trust or use.

This thesis examines how big data analytics supports enterprise decision-making, the main stages through which raw data becomes managerial insight, and the governance conditions required for analytics to improve rather than complicate decisions.

Main Part

From data accumulation to analytical value

Big data analytics can support descriptive, diagnostic, predictive and prescriptive decision-making. Descriptive analytics explains what has happened; diagnostic analysis explores why it happened; predictive models estimate what may happen next; and prescriptive approaches compare possible actions. These layers should be treated as complementary rather than as a maturity ranking that every organization must follow mechanically.

The business value of analytics appears when an analytical result is connected to a decision. A demand forecast matters when it changes purchasing or production; a fraud score matters when it changes transaction review; a customer model matters when it changes service or marketing. Analytics projects should therefore begin with a decision problem and measurable outcome rather than with data availability alone.

Analytics type	Typical question	Enterprise application
Descriptive	What happened?	Dashboards, performance reporting
Diagnostic	Why did it happen?	Root-cause and variance analysis
Predictive	What is likely to happen?	Demand, risk and failure forecasting
Prescriptive	What action should be taken?	Optimization and scenario selection

Data architecture and governance

Enterprise analytics requires consistent data definitions, metadata, access rules and quality controls. If different departments define customers, revenue, incidents or risk events differently, analytical outputs can become technically sophisticated but managerially disputed. A shared data architecture reduces this problem by clarifying sources, ownership and transformations.

Security and privacy are equally important. NIST's Big Data Interoperability Framework treats security and privacy as architectural concerns rather than afterthoughts. Access should be proportional to role and purpose, sensitive fields should be protected, and organizations should maintain traceability so that important analytical outputs can be linked back to their data sources.

Applications to risk management and engineering

Big data analytics is particularly relevant to risk management because many risks are dynamic and cannot be assessed adequately through periodic manual reporting alone. Transaction streams can support fraud detection, operational logs can identify unusual system behaviour, and historical loss data can improve scenario analysis. In engineering environments, sensor and maintenance data can support predictive maintenance and reliability analysis. However, data-driven decisions should not eliminate professional judgment. Models are based on historical relationships and assumptions that may change. Managers should understand the limitations of the data, monitor model performance and retain escalation mechanisms for unusual cases. The objective is

augmented decision-making: combining analytical scale and consistency with human contextual understanding.

Expanded Discussion: Building an Enterprise Analytics Pipeline

Reliable analytics begins before statistical modeling. Data must be captured from operational systems, checked for quality, transformed into consistent definitions and made available through controlled interfaces. When these steps are undocumented, managers may receive conflicting results from different dashboards even when analysts are using technically correct methods.

Metadata and lineage improve trust by showing where a measure originated and how it was transformed. This is especially important for financial and risk indicators, where a change in source data or calculation logic can alter a management conclusion. Traceability also makes analytical systems easier to audit and maintain.

Once the data foundation is stable, enterprises can select analytical techniques according to the decision problem. Forecasting is appropriate when future demand or risk needs to be estimated; anomaly detection is useful when rare deviations matter; optimization is valuable when managers must allocate constrained resources. The technique should follow the decision requirement rather than technology fashion.

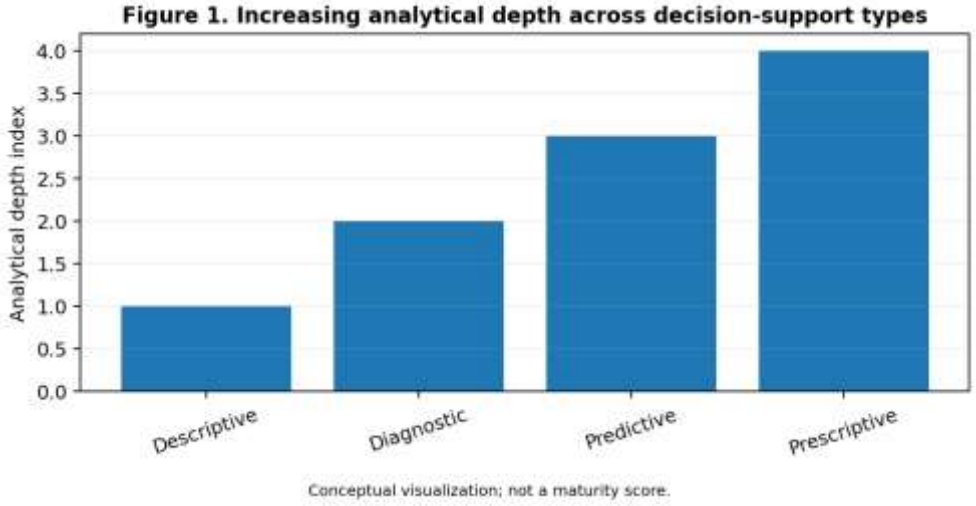


Figure 1. Increasing analytical depth across decision-support types.

Expanded Discussion: Decision Quality, Bias and Human Judgment

More data does not automatically produce better decisions. Historical datasets can contain missing values, inconsistent definitions and patterns created by earlier organizational choices. Predictive models may reproduce these patterns without understanding whether they remain appropriate. Managers should therefore examine data quality, representativeness and the operational meaning of variables before relying on model outputs. Human judgment remains important when decisions involve incomplete information, strategic change or unusual events. Analytics is strongest when

it narrows uncertainty and makes assumptions visible. Managers can compare model results with domain knowledge, scenario analysis and risk appetite instead of treating a prediction as a guaranteed outcome.

Decision quality should be evaluated after implementation. Organizations can compare forecast accuracy, processing time, loss rates, service levels or other relevant outcomes with a pre-implementation baseline. Feedback from these results can then improve both the analytical model and the business process.

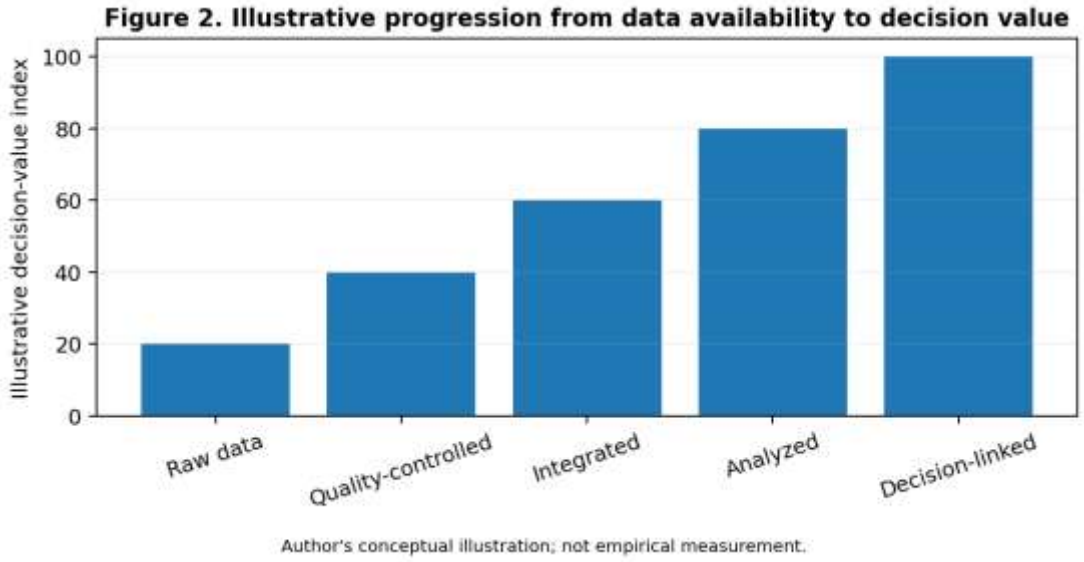


Figure 2. Illustrative progression from data availability to decision value.

Expanded Discussion: Governance for Sustainable Analytics

Data governance defines ownership, permitted use, access rights and quality responsibilities. Without it, analytics teams may spend substantial time locating and reconciling information rather than analyzing it. Governance should be practical and connected to business processes, with named data owners and clear procedures for correcting important data-quality problems. Security, privacy and model monitoring should continue after deployment. Access patterns change, source systems are updated and business conditions shift. A model that performed well during development may become less reliable if the underlying environment changes. Periodic validation and performance monitoring therefore protect decision quality as well as technical integrity.

For risk-management and engineering applications, governance should also preserve the ability to explain important outputs to decision makers. Documentation of data sources, assumptions, model versions and limitations allow managers to challenge results constructively and supports accountability when analytical recommendations influence material decisions.

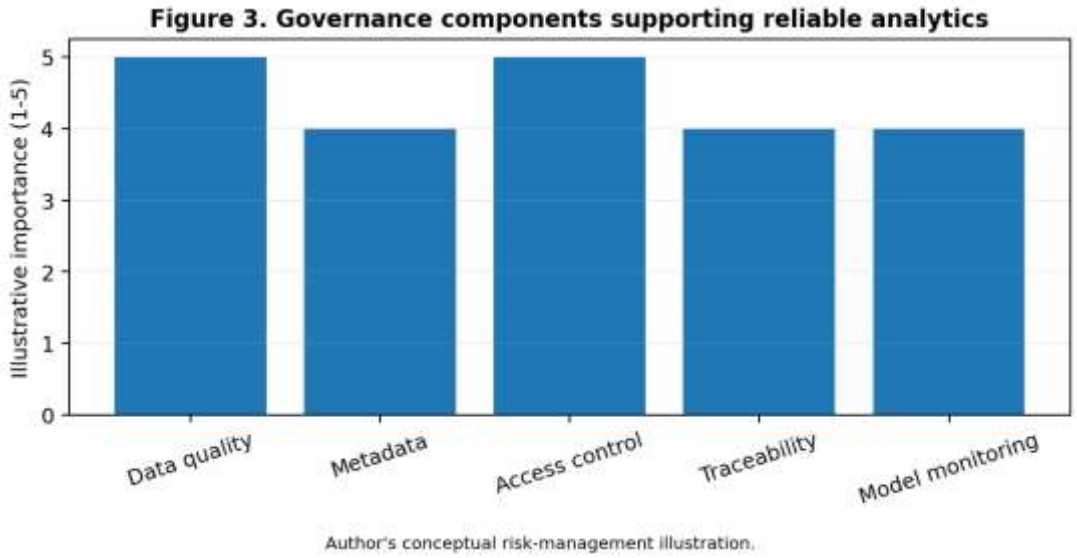


Figure 3. Governance components supporting reliable analytics.

Specific Enterprise Scenario: Analytics for Operational Risk and Predictive Maintenance

A more specific application can be built around operational risk and predictive maintenance. An enterprise can combine equipment sensor readings, maintenance history, incident records and work-order data in a governed analytical platform. Descriptive analytics reports failure frequency and downtime; diagnostic analysis compares failures with operating conditions; predictive models estimate the probability of failure within a defined time horizon; and the final decision rule can prioritize inspection when predicted risk and business criticality exceed agreed thresholds.

This workflow illustrates why data lineage matters. A maintenance-risk score should be traceable to source systems, transformations and model versions. If sensor calibration changes or a maintenance code is redefined, analysts need to know which reports and models are affected. The NIST Big Data Reference Architecture is useful here because it provides a vendor-neutral conceptual model with defined roles, activities and security/privacy and management fabrics (Chang, Boyd, & Levin, 2019).

Performance should be evaluated with operational measures rather than abstract claims about 'better decisions'. Suitable indicators include unplanned downtime, mean time between failures, false-positive maintenance alerts, average time from alert to inspection, maintenance cost per asset and the share of critical failures detected in advance. A model should be retained only if it improves relevant outcomes after considering its operating cost and error consequences.

Evidence and Governance Implications

NIST's Big Data Interoperability Framework treats large-scale data systems as an architectural problem involving providers, consumers, application functions, framework services, management and security/privacy. This supports a governance approach in which analytics is not separated from the systems that generate, transform and protect

data. For enterprises that extend analytics with AI, the 2025 OECD/BCG/INSEAD evidence is also relevant because it shows that adoption is connected with complementary capabilities, including cloud computing and skills. The implication for decision analytics is practical: a predictive model should be evaluated together with the data platform, workforce capability and process into which it is deployed, rather than as a standalone algorithm.

Conclusion

Big data analytics improves enterprise decision-making when it is organized around concrete decisions, supported by reliable architecture and governed throughout the data lifecycle. The progression from raw records to descriptive, predictive and prescriptive insight can shorten decision cycles and improve consistency, but only when managers trust the underlying data and understand the limitations of analytical models.

For enterprises, the practical priority is therefore not to collect the maximum possible amount of data. It is to build a controlled data environment in which relevant information can be accessed, analyzed and translated into accountable action.

Adabiyotlar, References, Литературы:

1. Chang, W., Boyd, D., & Levin, O. (2019). NIST Big Data Interoperability Framework: Volume 6, Reference Architecture. NIST SP 1500-6r2. https://doi.org/10.6028/NIST.SP.1500-6r2

2. NIST Big Data Public Working Group. (2019). NIST Big Data Interoperability Framework, Version 3.0 Final. National Institute of Standards and Technology.

3. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST SP 800-145. https://doi.org/10.6028/NIST.SP.800-145

4. Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1

5. OECD/BCG/INSEAD. (2025). The Adoption of Artificial Intelligence in Firms: New Evidence for Policymaking. OECD Publishing. https://doi.org/10.1787/f9ef33c3-en

6. Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29