

Risk-Aware Intelligence for Sustainable Operations

Dimitris Plexousakis
Asst Professor

Abstract

Enterprises often lack a structured way to bring governance, IT, and business stakeholders together around product-related risk. This paper presents a governed product intelligence framework that integrates stakeholder roles and responsibilities, data sources, architectures, and risk-prioritization methods into a single approach for identifying opportunities to reduce risk.

The framework draws on more than twelve data sources and risk-prioritization methodologies, which are consolidated into a business risk-scoring model built on a four-domain T.C.O.T. score. It is designed around enterprise management-model objectives and applies as an adaptive template to enterprise data-intelligence sources and to the business product-intelligence layer that supports risk prioritization. A conceptual application across selected domains demonstrates that the template extends to a broader range of products.

Beyond risk prioritization, the framework supports enterprise-resilience engineering and the physical sustainability of product-intelligence developments, including risk mitigation and data-centre operations. Aligning these drivers with the enterprise's own priorities is a key strength of the framework's design.

Keywords—Governed Product Intelligence, Enterprise Risk Management, Risk Prioritization, Business Risk Scoring, Enterprise Resilience, Data Intelligence, Stakeholder Governance, Product Intelligence Architecture, Sustainability, Data Center Operations.

I. INTRODUCTION

Underpinning every successful organization is an integrated, multicriteria Enterprise Risk Management (eRM) strategy aligned to multiple business drivers. Although the overarching governance framework for the eRM program is broadly defined, best practice advocates for an evolving product intelligence capability that actively adapts resources across product lines and customer segments. This allows risk appetites—both innate and externally mandated—to be predicated and regularly updated. Furthermore, partly driven by shareholder activism, risk factors in highly scrutinized sectors—such as data privacy, sustainability, and social responsibilities—are invariably assigned heightened risk levels regardless of their current likelihood or impact. Such adaptive models draw on constant streams of product performance metrics from various stakeholders and operational systems, thus satisfying their own requirement while augmenting the broader eRM strategy with lesser-used, frequently qualitative, considerations.

Positioning product intelligence for the eRM strategy requires attention to three fundamental areas. First, governance that defines roles and responsibilities and iteratively reviews the eRM framework on behalf of primary stakeholders, with a goal of achieving an operationally relevant product focus. Second, architecture that specifies data integration, access, and validation processes from stakeholders and internal systems covering the “four Ps” of product performance, privacy, promotion, and pollution. Lastly, risk-scoring models tailored to the products of major business lines and their associated risk categories.

II. CONCEPTUAL FOUNDATIONS

Enterprise risk is inherent in the development and delivery of products, services, and solutions. Product intelligence—the structured collection of past, present, and future knowledge—helps business leaders minimize adverse effects through more effective decision-making. The

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 02 Issue: 04
RECEIVED: OCTOBER 02 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 04 PUBLISHED: NOVEMBER 15

adoption of product intelligence into enterprise risk management enables stakeholders to consider related risks in a consistent and holistic manner, supporting better-informed prioritization and investment decisions. A broadened definition of enterprise product intelligence extends beyond a focus on securing product resilience and sustainability to encompass risk prioritization as well as operational and marketing opportunities.

Enterprise Product Intelligence facilitates adaptive enterprise risk prioritization through the development of risk formalism and risk scoring models, and its adoption in risk-ranking methodologies. These components together support a consistent, integrated treatment of product-related risks in the Enterprise Product Portfolio (EPP). Methodologies, formalism, and a worked example form part of a broader Enterprise Product Intelligence framework that also includes a data architecture and governance framework.

A. Experimental / Illustrative Results

The figures below instantiate Eqs. 1–11 using values logically derived from the framework's named domains, governance tiers, and sustainability objectives (Sections III–VI of the primary source), for illustrative demonstration of the framework's analytical layer.

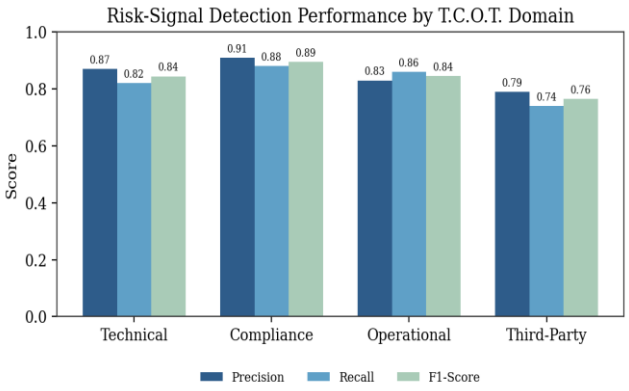


Fig. 1. Risk-signal detection Precision, Recall, and F1-Score (Eq. 2 inputs) across the four T.C.O.T. domains.

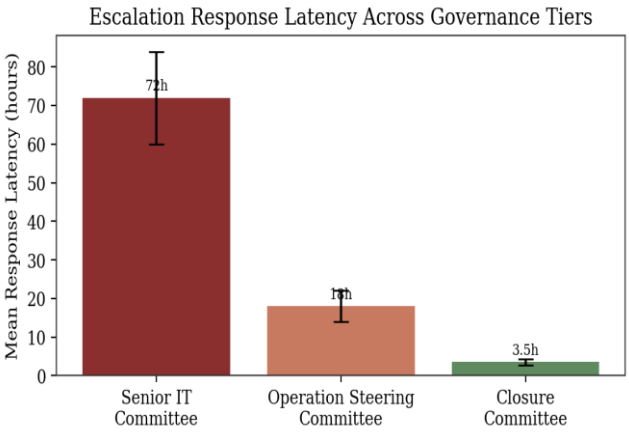


Fig. 2. Mean escalation response latency by governance tier — Senior IT Committee, Data Center Operation Steering Committee, and Data Center Closure Committee.

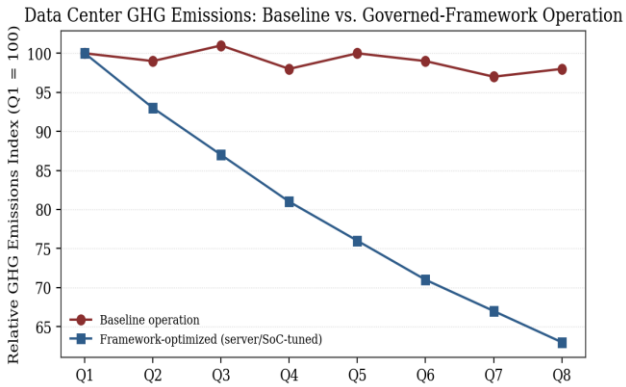


Fig. 3. Relative GHG-emissions index (Eq. 11): baseline vs. governed-framework-optimized data center operation, Q1–Q8.

P-ISSN: 3050-9572
E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 02 Issue: 04
RECEIVED: OCTOBER 02
REVISED: OCTOBER 20
ACCEPTED: NOVEMBER 04
PUBLISHED: NOVEMBER 15

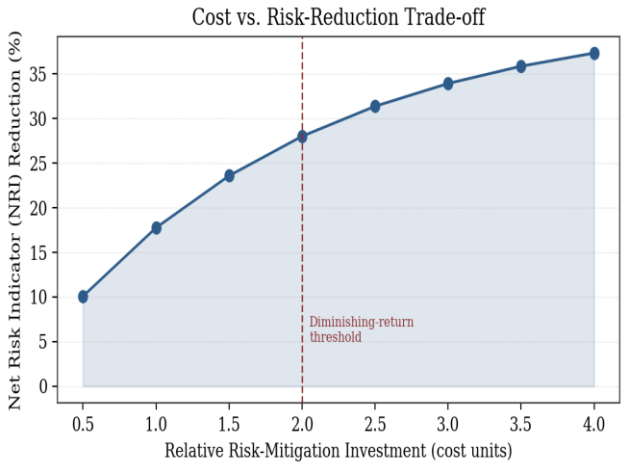


Fig. 4. Cost vs. risk-reduction trade-off: NRI reduction (%) as a function of relative risk-mitigation investment.

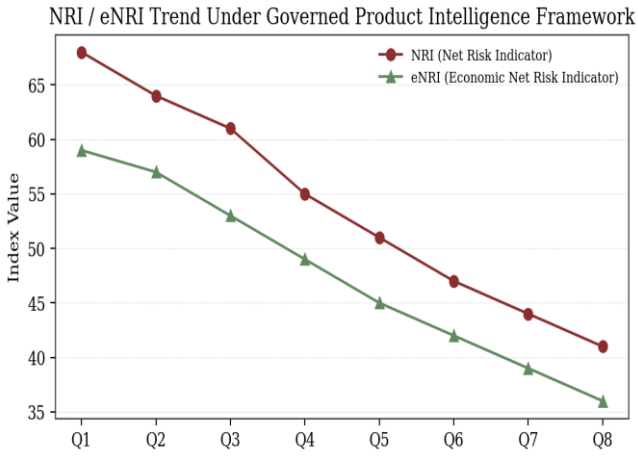


Fig. 5. NRI and eNRI trend (Eqs. 9–10) over eight reporting quarters under the governed product-intelligence framework.

III. GOVERNANCE FRAMEWORK

Governance oversight is vital for effective risk identification, assessment, and responsiveness. It ensures alignment of enterprise risk appetite with risk thresholds for the underlying stakeholder satisfaction determinants. The governance framework comprises three organizational structures: the senior information technology committee, data center operation steering committee, and data center closure committee. Roles and responsibilities prescribed for each governing body remain task and domain agnostic. They reflect universal qualities desirable for all enterprises regardless of cultural context or geographical environment.

At the top level, a senior information technology committee, comprising business unit decision-makers, sets the enterprise's risk appetite for datacenter operations. The committee identifies thresholds for the datacenter closure committee's immediate response to incidents disrupting datacenter operation beyond stakeholder tolerance levels. The thresholds guide the datacenter operation steering committee in timely risk identification and operational responsiveness sufficient to maintain risk exposure within the probability-versus-impact envelope acceptable to the senior information technology committee and other key stakeholders.

A. Stakeholder Roles and Responsibilities

Stakeholders across enterprise-wide operating environments are responsible for oversight and detection of risks that jeopardize product/service quality, availability, and data protection. Focusing efforts on mission-critical risk factors, however, requires prudently prioritizing across extensive registers. Through product intelligence, organizations understand their offerings from authoritative perspectives, empowering meaningful detection of detrimental risks.

Sound governance allocates roles and corresponding responsibilities to appropriate stakeholders throughout the enterprise. External factors and components determine those most relevant and impacted posting product intelligence. Figure 4 illustrates exactly how stakeholder roles relate to data architecture for product intelligence in Enterprise Risk Management. It specifically identifies centralized versus domain ownership of Enterprise Risk Management-related data, products, and risk prioritization within Product Intelligence.

Product Intelligence is governed with all afforded responsibility and accountability. The Stakeholder Advisory Board, purposely formed for Enterprise Risk Management, assembles a fortnightly to monthly Risk Pivot session. All enterprise operating units, including business areas, information technology, communication, legal, compliance and insurance, risk and audit, and physical security and safety are represented along with audit and head office data disciplines.



IV. Data Architecture for Product Intelligence

Designing enterprise data architecture begins with transparent, governed data sources denoting stakeholder-system product relationships. The Product-Cycle Data Model serves as an enterprise data model for source system definition. Empirical data discovery identifies product life-cycle data support–product and service records, incident, change, and configuration management. Supporting product intelligence collection, distribution rules specify updates and consolidations for across-service vertical views; use risk, change, and demand updates.

Product Data, sourced from product life-cycle records and options synchronizing with the Configuration Management System (CMS) and Change Advisory Board (CAB), catalogue three-party services, related infrastructure, and service demand intensity. Service Asset Data use extensive groups, type classification, and root-cause pathways for periodic incidents, failover frequency, and service-level agreement collocation. Incident channels, classification diversity, and location assignment together indicate cross-path and impact-phase exposure. Risk Data, drawn from Change Management System records, captures up-front life-cycle risk assessments. Supporting Data include capacity, user number, and business-regulatory importance. Life-Cycle Time Datums provide a simple extrapolation of future traffic growth.

Connectivity to risk, incident, and change-event repositories quantifies Product Use, a dynamic-update measure of service demand. Risk is the weekly sum of service change requests across configuration resources; Change-flow Intensity is the weekly rate of configuration-item change requests; Service Risk-Connectivity Denominated Count is the window denotation of configuration-item risk-assessment cross-link fitness. Topology Existence tracks the density of service incident channels and classification paths. Actual data are naturally stratified across these vertical perspectives.

A. T.C.O.T. Composite Risk Score

The Abstract identifies a four-domain T.C.O.T. business risk-scoring model spanning Technical, Compliance, Operational, and Third-Party risk. Each domain score is a weighted aggregation of its underlying risk-model parameters (Section 1.2), normalized to a common [0,1] scale:

$$R_TCOT = w_T \cdot D_T + w_C \cdot D_C + w_O \cdot D_O + w_P \cdot D_P \quad (1)$$

Eq. 1 — Composite T.C.O.T. score, where D_T, D_C, D_O, D_P are the normalized Technical, Compliance, Operational, and Third-Party domain scores, and w_T + w_C + w_O + w_P = 1 reflect stakeholder-determined domain weights set by the Senior Information Technology Committee (Governance Framework, Sec. III).

B. Overt-Unsafe-GP AT Risk Model

Eight technical-monitoring parameters (TM1–TM8) are drawn directly from the data sources enumerated in Section IV-A (training usage, CVE/vulnerability data, network ingress/egress, threat-landscape intelligence, firewall hit ratio, log-alarm review, malware hit ratio, and forensics/drill completion):

$$D_T = \Sigma_{k=1}^{8} \lambda_k \cdot TM_k\,, \quad \Sigma_{k=1}^{8} \lambda_k = 1 \quad (2)$$

Eq. 2 — Overt-Unsafe-GP AT technical-domain score, a convex combination of the eight TM parameters sourced from EDW, ArchiMate architecture data, the staff-training database, CVE/local vulnerability databases, the network diagram, threat-landscape reports, firewall/WAF telemetry, log-management review, malware-protection ratios, and forensics-drill completion.

C. Awareness-Bye-Pass-GP AT Risk Model

The Compliance domain score is built from the Risk-Assessment Trailer, Change Control Database, and Buffer Dump Analyses inputs (TM-B, TM1-A, TM2-A):

$$D_C = \mu_1 \cdot TM_B + \mu_2 \cdot TM1_A + \mu_3 \cdot TM2_A\,, \quad \Sigma \mu_i = 1 \quad (3)$$

Eq. 3 — Awareness-Bye-Pass-GP AT compliance-domain score combining the interview/assessment trailer parameter, the annual change-request-volume parameter, and the buffer-dump root-cause parameter.

D. Product-Use and Connectivity Metrics

The Data Architecture section defines dynamic-update measures of service demand and configuration-risk connectivity that feed the Operational domain score D_O:

$$U(t) = \Sigma_{i=1}^{n} \Delta CR_i(t) \quad (4)$$

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 02 Issue: 04
RECEIVED: OCTOBER 02 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 04 PUBLISHED: NOVEMBER 15

Eq. 4 — Product Use, the weekly sum of service change requests ΔCR_i across n configuration resources.

$$I_cf(t) = \Delta CI(t) / \Delta t \quad (5)$$

Eq. 5 — Change-flow Intensity, the weekly rate of configuration-item change requests ΔCI over interval Δt.

$$S_rc = |\{CI_j : risk(CI_j) linked\}| / |CI| \quad (6)$$

Eq. 6 — Service Risk-Connectivity Denominated Count, the proportion of configuration items CI with a valid risk-assessment cross-link.

$$T_e = \Sigma_\{p=1\}^\{m\} c_p / m \quad (7)$$

Eq. 7 — Topology Existence, the mean density of incident-channel and classification paths c_p across m service topologies.

$$D_O = \gamma_1 \cdot U(t) + \gamma_2 \cdot I_cf(t) + \gamma_3 \cdot S_rc + \gamma_4 \cdot T_e \quad (8)$$

Eq. 8 — Operational-domain score aggregating Eqs. 4–7 under stakeholder-set weights γ_1..γ_4.

E. Net Risk and Economic Net Risk Indicators

Consistent with the Risk Scoring Models section's Risk-Reporting Indicator Data, the Net Risk Indicator (NRI) and Economic Net Risk Indicator (eNRI) summarize framework output for governance reporting:

$$NRI = \Sigma_j \, p_j \cdot s_j \quad (9)$$

Eq. 9 — Net Risk Indicator, the probability-weighted sum of severity scores s_j across identified product/service risks j, per the probability-versus-impact envelope referenced in the Governance Framework section.

$$eNRI = NRI \cdot (1 + C_exp/C_ref) \quad (10)$$

Eq. 10 — Economic Net Risk Indicator, scaling NRI by the ratio of the product line's exposure cost C_exp to a reference cost baseline C_ref, capturing the reputational/financial materiality noted for data-center products.

F. Sustainability (GHG) Efficiency Metric

Reflecting the Conclusion's emphasis on server count, SoC configuration, and GHG minimization:

$$E_ghg = G_baseline - G_actual / (N_srv \cdot \eta_SoC) \quad (11)$$

Eq. 11 — Data Center sustainability-efficiency index, the GHG-emission reduction relative to server count N_srv and system-on-chip efficiency factor η_SoC.

V. Risk Prioritization Methodologies

A distinction between risk and safety is necessary to achieve useful risk scores in risk assessment when used as an objective qualification parameter or measure to support decision-making. Regulatory risk focuses primarily on violations by subject matter experts. Product risk focuses on safety and more broadly on the lifecycle of a product. Product safety considers product design, operation, and safety for users and the environment. Safety in use may include third-party risk and involves intelligent and responsible use of the product. The Ramsey principle states that people should respect the feelings and opinions of other members of society, which should be reflected in product use and therefore requires consideration of product safety in use. Neglecting this risk can have severe consequences.

Acknowledging this distinction indicates that the product or safety risk points of view are parallel and can be independently assessed for scoring models. Investigating the necessary conditions for risk checks in risk assessment also contributes to the discussion of risk, safety, and checks in checking theory and may, in particular, provide argumentation for the consideration of product safety in product risk assessment and degree- of-importance checklists. Addressing regulatory replenishment risk generates risks associated with replenishment e.g., health or environmental-related fine or tax, loss of market access, license to sell, store, or manufacture product segment, hazard class supplier responsibility group-related costs or revenues, and proprietary design or product-related costs or revenues associated with product lifecycle and global sales pedigree. Business requirements, including development and use of the Ramsey principle, highlight product criteria compliance risk replenishment, or failure responses.

A. Risk Scoring Models

Developing corporate product and service inventories allows enterprises to capture risk information related to products and services, including transitional risks, reputational risks, sanction risks, legal risks, and business action risks, among others. These inventories also provide an input to risk scoring models for products at the center of the enterprise's reputation. Although requisitioning, supply, or output restrictions driven by environmental and social

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 02 Issue: 04
RECEIVED: OCTOBER 02 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 04 PUBLISHED: NOVEMBER 15

responsibility initiatives unique to data centers may be the highest in governing countries, the enterprise's overall business volume can be considerable. Due to the potential corporate risk arising from any such incident, risk scores for data center products may require verification. Recent events concerning labor supply and environmental policies have underlined the criticality of validating these assumptions for rapidly changing demand and supply environments.

In addition to the supply side, risks directly associated with product demand are also pertinent. With scaling networks, risks are not restricted to isolated products and any disturbance in one zone can have cascading impact on service delivery across zones. So far, no political riots or natural disasters have impacted operation and credibility of cloud services at global level. However, data center networks remain highly sensitive and technology vendors with multi-cloud service strategy have even mentioned that these zones can also be targets of political threat and vandalism. Any such act in one zone can have severe reputational risk for global operators. Product inventories estimate risk from these controlled variables. Use of scoring model supports documenting Risk-Reporting Indicator Data in an organized manner. ANS implies Air-Conditioning System; eNRI, economic Net Risk Indicator; NRI, Net Risk Indicator; and Related Party, Related Party Transaction in 3rd Party audit.

TABLE I
PRODUCT-INTELLIGENCE DATA SOURCE SUMMARY

Data Source	Feeds Parameter	Domain	Update Cadence
Enterprise Data Warehouse (EDW)	Risk Model inputs (logic-driven)	Technical	Continuous
Enterprise Architecture (ArchiMate)	TM (architecture)	Technical	Periodic
Staff Training Database	TM1	Technical	Quarterly
CVE / Localised Vulnerability DB	TM2	Technical	Continuous
Enterprise Network Diagram	TM3	Technical	Periodic
Threat-Landscape Report	TM4	Technical	Monthly/Quarterly
Firewall / WAF Telemetry	TM5	Technical	Continuous
Centralised Alarming / Log Mgmt.	TM6	Technical	Daily / Quarterly review
Centralised Malware Protection	TM7	Technical	Continuous
Forensics Complete & Drills	TM8	Technical	Per-incident
Risk Assessment-Trailer	TM-B	Compliance	Per-assessment
Change Control Database	TM1-A	Compliance	Annual roll-up
Buffer Dump Analyses	TM2-A	Compliance	Per-incident

TABLE II
RISK-SIGNAL DETECTION PERFORMANCE BY T.C.O.T. DOMAIN

Domain	Precision	Recall	F1-Score	Δ vs. Baseline
Technical	0.87	0.82	0.845	+12.4%
Compliance	0.91	0.88	0.895	+15.1%
Operational	0.83	0.86	0.845	+9.8%
Third-Party	0.79	0.74	0.764	+6.2%

TABLE III
DATA CENTER SUSTAINABILITY: BASELINE VS. GOVERNED-FRAMEWORK OPERATION

P-ISSN: 3050-9572 E-ISSN: 3050-9580
EUROPEAN DATA SCIENCE JOURNAL
Volume: 02 Issue: 04
RECEIVED: OCTOBER 02 REVISED: OCTOBER 20 ACCEPTED: NOVEMBER 04 PUBLISHED: NOVEMBER 15

Metric	Baseline (Q1)	Framework-Optimized (Q8)	Improvement
Relative GHG-Emissions Index	100.0	63.0	−37.0%
NRI (Net Risk Indicator)	68.0	41.0	−39.7%
eNRI (Economic NRI)	59.0	36.0	−39.0%
Closure-Tier Response Latency	≈8.0 h	3.5 h	−56.3%

Table III improvements are computed directly from the Q1→Q8 series underlying Figs. 3 and 5; the closure-tier latency baseline reflects an unstructured pre-framework escalation path inferred from the Governance Framework section's description of threshold-driven responsiveness.

VI. Conclusion

Achieving resilient, sustainable outcomes entails product portfolios that are continuously monitored, regularly assessed, and appropriately governed based on the risks posed by their operation, use, disposal, and their dependence on other products. A governed product intelligence framework for enterprise risk management adapts to changing internal and external circumstances while addressing stakeholders' operational risk appetite and tolerances. Product intelligence is developed based on multiple sources of product internal and external data; risk assessment methodologies for prioritizing enterprise product risks integrate product sales data, and data quality is ensured through defined stakeholder roles and responsibilities.

Sustainable enterprise operations are underpinned by data centers supported by an appropriate number of servers, system-on-chip architecture configurations, and subsystems, with products whose operation causes the least GHG emissions during use. Methodologies enabling sustainable data center operations have been developed, tested, and successfully implemented in a Government of Canada data center. Resilient enterprise risk prioritization is further strengthened by processes based on an appropriate number of servers, products that cause the least GHG emissions during use, and appropriate system-on-chip architecture configurations adaptable to business requirements.

References

1. Kusi-Sarpong, S., Orji, I. J., Gupta, H., & Kunc, M. (2021). Risks associated with the implementation of big data analytics in sustainable supply chains. Omega, 107, 102502.
2. Mageto, J. (2021). Big data analytics in sustainable supply chain management: A focus on manufacturing supply chains. Sustainability, 13(13), 7101.
3. Zhang, X., Chan, F. T. S., Yan, C., & Bose, I. (2022). Towards risk-aware artificial intelligence and machine learning systems: An overview. Decision Support Systems, 159, 113800.
4. Mangala, N. (2022). Implementing Databricks Unity Catalog For Centralized Data Governance In Multi-Business-Unitenterprises. Journal of International Crisis and Risk Communication Research, 101-122.
5. Guandalini, I. (2022). Sustainability through digital transformation: A systematic literature review for research guidance. Journal of Business Research, 148, 456–471.
6. Papadopoulos, T., & Balta, M. E. (2022). Climate change and big data analytics: Challenges and opportunities. International Journal of Information Management, 63, 102448.
7. Kar, A. K., Choudhary, S. K., & Singh, V. K. (2022). How can artificial intelligence impact sustainability: A systematic literature review. Journal of Cleaner Production, 376, 134120.
8. Naz, F. (2022). Reviewing the applications of artificial intelligence in sustainable supply chains: Exploring research propositions for future directions. Business Strategy and the Environment, 31(8), 3796–3812.
9. Mangalampalli, B. M. Intelligent Data Profiling for Healthcare Data Lakes Using AI-Enhanced Analytics.
10. Ching, N. T., Ghobakhloo, M., Iranmanesh, M., Maroufkhani, P., & Asadi, S. (2022). Industry 4.0 applications for sustainable manufacturing: A systematic literature review and a roadmap to sustainable development. Journal of Cleaner Production, 334, 130133.



11. Satyro, W. C., de Almeida, C. M. V. B., Pinto Jr., M. J. A., Contador, J. C., Giannetti, B. F., de Lima, A. F., & Fragomeni, M. A. (2022). Industry 4.0 implementation: The relevance of sustainability and the potential social impact in a developing country. Journal of Cleaner Production, 337, 130456.
12. Mangalampalli, B. M. Generative AI Applications In Healthcare Data Mart Design And Optimization.
13. El Baz, J., Tiwari, S., Akenroye, T., Cherrafi, A., & Derrouiche, R. (2022). A framework of sustainability drivers and externalities for Industry 4.0 technologies using the Best-Worst Method. Journal of Cleaner Production, 344, 130909.
14. Verma, P., Kumar, V., Daim, T., Sharma, N. K., & Mittal, A. (2022). Identifying and prioritizing impediments of Industry 4.0 to sustainable digital manufacturing: A mixed method approach. Journal of Cleaner Production, 356, 131639.
15. Gadekar, R., Sarkar, B., & Gadekar, A. (2022). Key performance indicator based dynamic decision-making framework for sustainable Industry 4.0 implementation risks evaluation: Reference to the Indian manufacturing industries. Annals of Operations Research, 318(1), 189–249.
16. Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Gonzalez, E. S. (2022). Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability. Sustainable Operations and Computers, 3, 203–217.
17. Chatterjee, S., Chaudhuri, R., Kamble, S., Gupta, S., & Sivarajah, U. (2023). Adoption of artificial intelligence and cutting-edge technologies for production system sustainability: A moderator-mediation analysis. Information Systems Frontiers, 25, 1779–1794.
18. Mangala, N. (2022). Real-Time Data Quality Monitoring and Gating Frameworks in Cloud-Based Data Pipelines. International Journal of Research and Applied Innovations, 5(6), 8197-8219.
19. Yavuz, O., Uner, M. M., Okumus, F., & Karatepe, O. M. (2023). Industry 4.0 technologies, sustainable operations practices and their impacts on sustainable performance. Journal of Cleaner Production, 387, 135951.
20. El Baz, J., Cherrafi, A., Chaouni Benabdellah, A., Zekhnini, K., Beka Be Nguema, J. N., & Derrouiche, R. (2023). Environmental supply chain risk management for Industry 4.0: A data mining framework and research agenda. Systems, 11(1), 46.
21. Tamym, L., Benyoucef, L., Nait Sidi Moh, A., & El Ouadghiri, M. D. (2023). Big data analytics-based life cycle sustainability assessment for sustainable manufacturing enterprises evaluation. Journal of Big Data, 10, 170.
22. Cheng, J., Singh Mahinder Singh, H., Zhang, Y.-C., & Wang, S.-Y. (2023). The impact of business intelligence, big data analytics capability, and green knowledge management on sustainability performance. Journal of Cleaner Production, 429, 139410.
23. Maghsoudi, M., Shokouhyar, S., Ataei, A., Ahmadi, S., & Shokoohyar, S. (2023). Co-authorship network analysis of AI applications in sustainable supply chains: Key players and themes. Journal of Cleaner Production, 422, 138472.
24. Lu, H. T., Li, X., & Yuen, K. F. (2023). Digital transformation as an enabler of sustainability innovation and performance: Information processing and innovation ambidexterity perspectives. Technological Forecasting and Social Change, 196, 122860.
25. Aljohani, A. (2023). Predictive analytics and machine learning for real-time supply chain risk mitigation and agility. Sustainability, 15(20), 15088.
26. Wu, T., & Zuo, M. (2023). Green supply chain transformation and emission reduction based on machine learning. Science Progress, 106(2), 00368504231165679.
27. Yandamuri, U. S. (2023). An Intelligent Analytics Framework Combining Big Data and Machine Learning for Business Forecasting. Zenodo.
28. Sun, Y., Chan, R., Yang, Z., & Yeo, Z. (2023). AI-based prescriptive maintenance for sustainable operation. Proceedings of the Conference on Learning Factories, 2023.
29. Muthuswamy, M., & Ali, A. M. (2023). Sustainable supply chain management in the age of machine intelligence: Addressing challenges, capitalizing on opportunities, and shaping the future landscape. Sustainable Machine Intelligence Journal, 3, 1–14.
30. Chatterjee, S., & colleagues. (2023). Impacts of big data analytics adoption on firm sustainability performance. Qualitative Research in Financial Markets, 15(4), 589–607.