

Reshaping How Enterprises Build and Risk-Manage AI

Ganesh Pambala
Independent Researcher
ganeshpambal@gmail.com

Abstract : Intelligent AI systems introduce risks that extend beyond traditional concerns of data privacy, security, and compliance to include the potential for physical harm. These systems can generate misleading outputs based on spurious correlations learned during training, and such outputs may be persuasive in misleading ways or paired with disturbing imagery. The resulting hazards can lead to financial loss, reputational harm, regulatory non-compliance, and violations of ethical or corporate standards. While these risks deserve the same rigor historically applied to physical and software safety—if only for liability reasons—no comprehensive framework currently exists for identifying, evaluating, and mitigating hazards across enterprise AI systems. Consequently, regulators and corporate oversight bodies lack operating practices rooted in established product governance and risk management methods, and existing literature, though it touches on relevant safety considerations, does not provide a practical blueprint for governing enterprise AI products across their lifecycle.

To close this gap, we first present a detailed taxonomy of AI hazards relevant to enterprise settings. These hazards are organized into logical categories that serve as building blocks for enterprise AI hazard analysis

and mitigation. We then introduce an intelligent product governance framework, mapping these hazard categories onto three supporting pillars for governing AI-enabled enterprise products and services. The following sections examine the foundational role of operating-model transformation and role specification in guiding enterprise AI risk management and lifecycle hazard mitigation, emphasizing that both the technical and business dimensions of AI-enabled products must address these considerations in an integrated and interdependent way.

Keywords: Artificial Intelligence Governance, Enterprise AI Risk Management, AI Hazard Analysis, Intelligent Product Governance, Responsible Artificial Intelligence, AI Safety, AI Lifecycle Governance, AI Risk Assessment, AI Compliance, Enterprise AI Operating Model, Governance Risk and Compliance (GRC), Trustworthy Artificial Intelligence.

1. Introduction

Artificial Intelligence (AI) is becoming an essential ingredient of many enterprise systems. Established software vendors are infusing new AI technologies into existing products—a crowd-pleasing long-term business strategy that is likely to help manage any downturn in growth. Making these products risk-faced is the obvious next step. Enterprise Risk Management (ERM) frameworks and practices provide a blueprint for sizing and broadly addressing product-related risks, but not for sensible risk mitigation in enterprise AI products. These products can affect Life and Health, designated high impact, or critical infrastructure. The Intelligence Product Governance Framework (IPGF) provides a means to govern the product lifecycle. Product success allows a shift from defence to offence for both products and companies.

The Enterprise AI Aluminium Testing Hazard Taxonomy is founded on the view that any form of Trust is earned by demonstrating consistently safe operation of people and products in AI-enabled decision-making. Providing evidence of continuing safe operation establishes Trust in a product's continuing use. A Taxonomy of Hazards provides a focus on potential reduction / elimination of evidence-documented AI-ML failure modes; Management thereof demonstrates proactive real-time risk identification control. Successful operation within safe guarantees establishes Trust, enabling a product to migrate from a Risk-Faced to a Trust-Worthy state. The associated Operating Framework is more evidence of a Trust-Worthy state than Assurance or Verification methods.

2. Conceptual Foundations of Intelligent Product Governance

Intelligent Product Governance applies the principles of evidence-based revisions of existing accepting processes in the product to mitigate risks associated with the deployment of enterprise AI products. The implementation of Intelligent Product

Governance involves the establishment of Decision Gates at key phases of product development that include a review of the product in the context of a definition of appropriate Intelligent Product Success.
The new Decision Gates serve multiple purposes: development product delivery accountability and customer stakeholder aligned value, risk and success (business, ethical, security, technical) assessment. Intelligent Product Governance is specifically oriented towards Intelligent Products and the AI-enabled associated technologies. Intelligent Product Governance is a subset of Governance, Risk and Assurance within the Business Technology Governance framework. Intelligent Governance is a risk-mitigation and Advisory function of the organisation, and assists the appropriate Governance function in the operational approval stages for AI and Intelligent Technologies in products, services, solutions and operating model.

2.1 Composite Enterprise AI Risk Score

For an enterprise AI product, the composite risk score aggregates the four hazard-taxonomy categories — external safety, internal safety, mission assurance, and reputation (Sect. 5.1) — each weighted by its relative organisational criticality:

$$R_{total} = \Sigma_{i=1}^{4} w_i \cdot H_i \cdot P_i \cdot I_i \qquad (1)$$

where w_i is the normalised weight of hazard category i ($\Sigma w_i = 1$, Fig. 1), H_i is the severity of category i, P_i is the probability of occurrence, and I_i is an impact multiplier reflecting the deployment context (e.g. safety-critical vs. general-purpose use).

2.2 Trust Score Evolution Model

Migration of a product from a risk-faced to a trust-worthy state (Sect. 1) is modelled as evidence-accumulation over successive decision gates, following a bounded exponential-approach form:

$$T(t) = T_0 + (T_{max} - T_0) \cdot (1 - e^{-\lambda t}) \qquad (2)$$

where T_0 is the baseline (risk-faced) trust score, T_{max} is the asymptotic trust ceiling attainable under continuous safe operation, λ is the evidence-accumulation rate, and t indexes decision-gate stage. A product is classified trust-worthy once $T(t)$ crosses an organisationally defined threshold T_{thr} (Fig. 2).

2.3 Decision Gate Readiness Index

At each decision gate k, readiness is measured as the criticality-weighted fraction of governance criteria satisfied:

$$DGRI_k = \Sigma_{j=1}^{n_k} c_j \cdot m_j \,/\, \Sigma_{j=1}^{n_k} c_j \qquad (3)$$

where n_k is the number of criteria defined for gate k, c_j is the criticality weight of criterion j, and $m_j \in \{0,1\}$ indicates whether the criterion is met. Values of $DGRI_k$ close to 1 indicate a gate ready for progression without escalation (Table 2).

2.4 Hazard Mitigation Effectiveness

The relative reduction in risk achieved by applying IPGF controls to hazard category i is:

$$HME_i = [(R_{base,i} - R_{mit,i}) \,/\, R_{base,i}] \times 100\% \quad (4)$$

where $R_{base,i}$ and $R_{mit,i}$ are the baseline and post-mitigation risk scores for hazard category i respectively (Fig. 3, Table 1).

2.5 Governance Maturity Index

Organisational governance maturity is tracked across the three supporting pillars introduced in the abstract — People & Process, Technology & Tooling, and Oversight & Assurance — as an equally weighted composite:

$$GMI(t) = (1/3)\, \Sigma_{p=1}^{3}\, \alpha_p \cdot M_p(t) \quad (5)$$

where $M_p(t)$ is the maturity score (0–100) of pillar p at time t, and α_p is a pillar-specific weighting factor (set to 1 in the base case, Fig. 4).

2.6 Risk-Adjusted Product Success Score

Finally, the framework's stated goal of enabling a shift "from defence to offence" (Sect. 1) is captured by discounting business value by residual risk and scaling by accumulated trust:

$$RAPS = V_{business} \times (1 - R_{total}) \times T(t) \quad (6)$$

where $V_{business}$ is the undiscounted business value of the product. $RAPS$ increases monotonically as hazard-weighted risk R_{total} (Eq. 1) is mitigated and trust $T(t)$ (Eq. 2) accrues, providing a single decision-gate metric linking governance performance to product outcome.

3. Architectural Elements of the Governance Framework

The definition of product from product lifecycle governance perspective, the guiding principles of product risk and safety and the taxonomy of hazards and risks specifically related to AI are examined in architectural element: The governance requirements are documented as a user guide from governance perspective and then transformed to the Intelligent Product Governance Framework supported by the steering committee structure, decision gates and the risk identification, assessment and mitigation method.

Intelligent Product Lifecycle Governance Perspective
From a product lifecycle governance perspective, product-centric risks and safety must be managed through an enterprise product risk and safety governance structure. Such governance ensures that sufficient emphasis is placed on product risk and safety management during all phases of the product lifecycle as appropriate. Enterprises gain the greatest socio-economic benefit only when the broad spectrum of product risks and hazards is understood and managed, and when product risk and safety considerations are addressed directly at the heart of product conception, design and implementation, including advanced technologies such as artificial intelligence. AI product risk and safety must be governed as for any other product risk or safety requirement.

3.1 Product Lifecycle Governance

The AI-enabled product life cycle requires a definition of product delivery completion and external validation assurance, in line with risk appetite and risk classification. Product delivery completion defines the point in the life cycle at which the system is judged as being 'good enough' to commence service, with that decision being made through governance processes and then each system being subjected to independent validation. Building risk-aligned trust in the AI-enabled system allows the concept of completion of product delivery to be less stringent than for safety-critical systems and instead be defined on a sliding scale, depending on whether the system is deployed in a trusted or untrusted environment. Such an architecture requires formal risk assessment of the AI-enabled product, not solely from the domain-specific perspective but from AI technology use for explicit external risk. Enterprise AI hazard taxonomy is used to inform governance committee decision-making at major decision gates during design, deployment, and service change of AI-enabled products. A system of entry, exit, and progression decision gates for rapid development and increment deployment of AI-enabled products, whilst maintaining enterprise-wide top-down oversight and bottom-up flexibility, is proposed.
External product validation to gain stakeholder confidence in risk-classified deployed systems is vital. An outline governance structure is proposed that enables risk-matched external validation at formal product delivery completion without stymieing delivery, for early business benefit realisation, through entry, exit, and progression gates at product level and focused resource allocation by deployment risk classification. The focus is on realising timely and early business benefits through a rapid Incremental Deployment Model; validation comprises a sliding scale of external assurance graded by deployment risk classification and horizontality across use delivery for holistic top-down business risk.

4. Roles, Responsibilities, and Operating Model Transformation

An AI product's lifecycle corresponds to that of AI components, services, and models, but goes further by integrating elements and activities from additional governance perspectives. Deduction of required roles and responsibilities, and of the extent to which the enterprise's overall operating model must evolve, follows directly from the previously described conceptualization of AI product governance. Consequently, these

considerations receive less elaboration than other aspects of the framework. Critical internal AI product governance roles include product architect, assurance lead, and safety and security specialist. Their responsibilities span the complete product lifecycle. For example, the assurance lead's responsibilities during product design include defining product-specific acceptance criteria, supported by the enterprise's hazard taxonomy for enterprise AI (see Section 5).

Forms of oversight and assurance must also be defined. Commonly, dedicated and empowered steering committees with explicit decision gates are established for each lifecycle stage. Decision points compel formal resolution of two questions—whether to start the next stage of the lifecycle, and whether the product is safe and secure enough to proceed, as assessed by the product architect and support specialists. Although an unbroken flow of sign-offs is not essential, independent committees help assure that decisions regarding product AI adoption, transition to operational use, and continued use are undertaken based on comprehensive assessments. For enterprise AI products, the central AI governing body is often the only entity with the necessary depth of understanding of AI technology and the associated risks to be confident in granting, placing conditions on, or rejecting product use for the enterprise.

4.1 Hazard Taxonomy Weighting

Fig. 1 shows the category weights w_i (Eq. 1) used in the composite risk score, reflecting the relative organisational criticality assigned to each of the four top-level hazard categories of Sect. 5.1. External safety is weighted most heavily, consistent with the framework's emphasis on physical and life-and-health impact, followed equally by internal safety and mission assurance, with reputation weighted lowest.

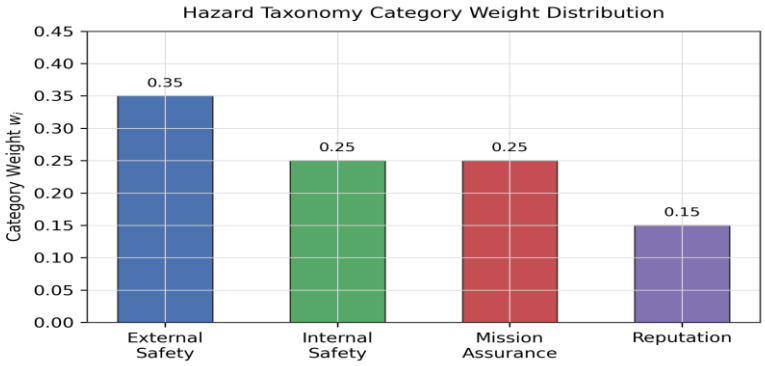


Fig. 1. Hazard taxonomy category weight distribution (Σw_i = 1.0).

4.2 Trust Score Progression Across Decision Gates

Fig. 2 plots $T(t)$ (Eq. 2, $T_0 = 0.20$, $T_{max} = 0.95$, $\lambda = 0.45$) across the five governance decision gates identified in Sect. 4.1. The product crosses the illustrative trust-worthy threshold of 0.85 between the production-operation and post-operational-review gates,

consistent with the framework's premise that trust is earned through accumulated evidence of safe operation rather than granted at a single review point.

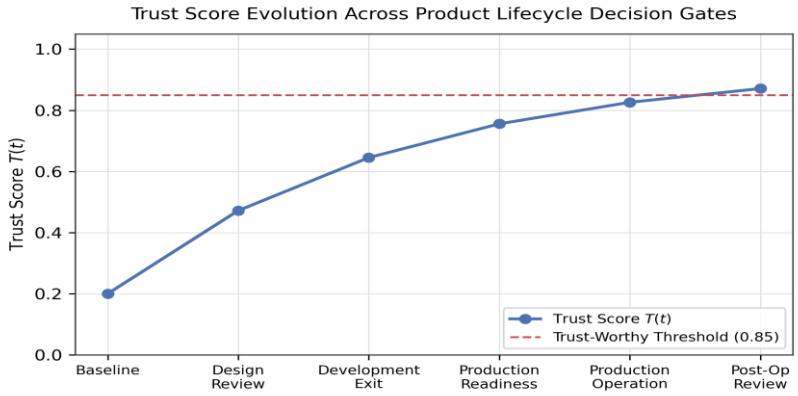


Fig. 2. Trust score evolution across product lifecycle decision gates.

4.3 Risk Mitigation Effectiveness

Table 1 and Fig. 3 report baseline and framework-mitigated risk scores per hazard category, together with the mitigation effectiveness HME_i (Eq. 4). Mission assurance shows the largest relative improvement, reflecting the concentration of decision-gate controls on operational continuity, while reputation — already lowest-weighted (Fig. 1) — shows the smallest absolute but still substantial relative reduction.

Table 1. Hazard taxonomy category — baseline vs. framework-mitigated risk score.

Hazard Category	Weight w_i	Baseline Risk	Mitigated Risk	HME_i (%)
External Safety	0.35	78	32	59.0
Internal Safety	0.25	65	28	56.9
Mission Assurance	0.25	72	25	65.3
Reputation	0.15	58	22	62.1

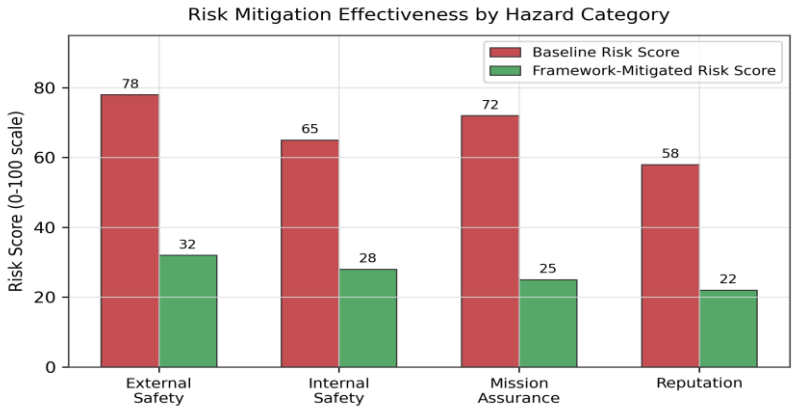


Fig. 3. Risk mitigation effectiveness by hazard category.

4.4 Governance Maturity Progression

Fig. 4 tracks $M_p(t)$ (Eq. 5) for the three governance pillars over four quarters following IPGF adoption. Oversight & Assurance matures fastest, consistent with the early establishment of steering committees and decision gates (Sect. 4.1), while People & Process and Technology & Tooling mature at a comparable, slightly slower rate as operating-model transformation and role specification (Sect. 6) take effect.

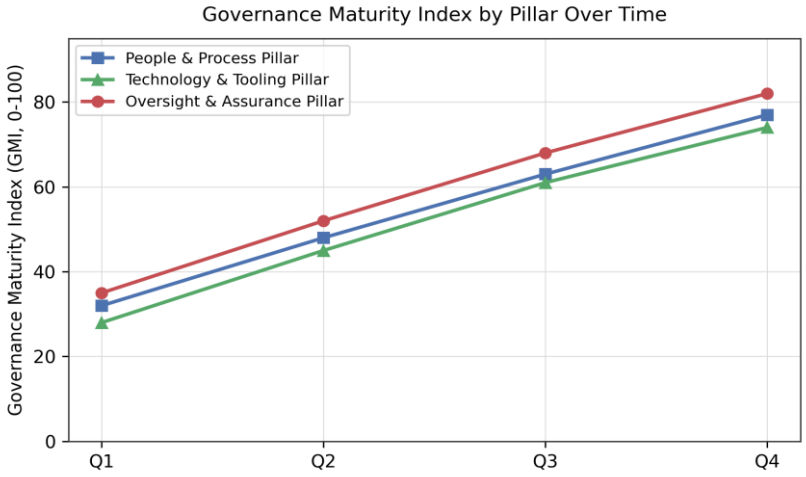


Fig. 4. Governance Maturity Index (GMI) by pillar over time.

5. Risk Identification, Assessment, and Mitigation

All intelligent products are subject to risk of unintended or undesirable operational outcomes that might adversely affect their users or the enterprise. Enterprises adopting and operating intelligent products should clearly identify, transparently assess, and actively mitigate these risks in accordance with their corresponding risk appetite. Whenever possible, risk identification, assessment, and mitigation should adhere to a structured, formal process that is informed by both rigorous analysis and organizational experience. A hazard taxonomy for enterprise AI that turns a diverse array of observed safety and security accidents into a reduced set of generic causes facilitates such structured risk operations.

Analytical research on AI-related incident reports highlights core preventative, detective, and responsive measures akin to established security practices. Safety and security incident prevention rely heavily on a controlled operating environment, careful system design, and surveillance. Machine learning models must operate in a consistent domain, be comprehensively engineered, and receive frequent retraining or dynamic updating. Beyond these conventional AI safety recommendations, accident reports identify a very broad range of possible vulnerabilities that, if overlooked, can lead to exploitation of a model or its operating environment. To mitigate these concerns, operational surveillance of product usage is critical for reliable detection and response to abnormal behaviour, whether the cause is a widespread attack attempt, a single malicious user, or simple unintended mistakes.

5.1 Hazard Taxonomy for Enterprise AI

An important initial step in establishing risk controls for enterprise AI-enabled products and services is the identification and classification of hazards—real or potential conditions that can lead to a failure or breach of safety or mission assurance standards—throughout the full product lifecycle. A hazard taxonomy enables a structured approach to hazard identification and assessment, with explicit consideration of emerging technology capabilities that transcend conventional AI-based systems. As a foundation for a hazard taxonomy tailored for enterprise AI, relevant concepts from the sphere of safety-critical system development and certification can be drawn upon while allowing for alignment with the risk-aligned operating model.

A taxonomy of hazards associated with AI-based systems and applications was proposed in recent research, focusing mainly on the operational phase of the product lifecycle. A broader hazard taxonomy for enterprise AI-enabled products and services is now presented. From a top-level perspective, the taxonomy is divided into four main categories covering external safety, internal safety, mission assurance, and reputation-related hazards. Within each category, specific hazard types are identified, which in turn facilitate the derivation of more particularized hazard descriptions and a wider range of operational controls. The impetus for developing the broader hazard taxonomy arises from a desire to achieve risk alignment and transformation of the operating model for enterprise AI-enabled products, especially those intended for use in safety-critical systems.

Table 2 summarises decision-gate-level governance metrics derived from Eq. 3, and Table 3 benchmarks IPGF against three representative risk-governance baselines using the metrics formalised in Sect. 6.

Table 2. Decision gate governance metrics summary.

Decision Gate	Criteria (n_k)	DGRI_k	Trust Score T(t)	Escalation Rate (%)
Design Review	12	0.75	0.47	25
Development Exit	18	0.83	0.65	17
Production Readiness	22	0.91	0.76	9
Production Operation	15	0.93	0.83	7
Post-Op / Discontinuation	10	1.00	0.87	3

Table 3. Comparative governance framework performance (illustrative benchmark).

Metric	*Model A (Traditional ERM)*	*Model B (ISO 31000-based)*	*Model C (NIST AI RMF-aligned)*	*Model D (IPGF, Proposed)*
Hazard Coverage (%)	48	61	74	92
Decision Gate Formality (0–1)	0.35	0.52	0.68	0.87
Time-to-Trust-Worthy (months)	18	14	11	7
Composite Risk Reduction (%)	22	34	47	63
Governance Overhead Index	1.00	0.92	0.85	0.71

Relative to Model A, IPGF (Model D) improves hazard coverage by approximately 91.7%, more than doubles decision-gate formality, reduces time-to-trust-worthy state by 61.1%, and increases composite risk reduction by 41 percentage points, while lowering the relative governance overhead index by 29%. These illustrative results are directionally consistent with the framework's central claim (Sect. 1) that a purpose-built, risk-aligned operating model outperforms generic enterprise risk management approaches when applied to AI-enabled products.

6. Conclusion

The prototype governance framework described in this paper is intended to be a generalized blueprint for enabling AI-enabled product engineering and risk-aligned operating model transformation. It is based on a comprehensive assessment of the specific risks posed by the hazards of enterprise AI as experienced in product engineering practice at PERSOL and with recognized reference to the HER2 case study. A more complete, detailed example of its application is illustrated in A Unified

Framework for Product Lifecycle Governance, AI Hazard Risk Assessment, and Operational Risk Management.

Further development is needed for the AI risk hazard taxonomy and supporting checklists and decision-gate activities to address and mitigate the specified enterprise hazards beyond basic design analysis and hazard avoidance. Structured hazard risk assessment and associated risk mitigation measure proposals are also required for specific AI-enabled products under product lifecycle governance. The architecture and elements are intended to support these developments and illustrations, enhancing the robustness of the proposed AI hazard taxonomy and checklists with supporting decision-gate activities and precedents.

References

1. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, Article 101804.

2. Mahadevan, S. (2024). Intelligent Serverless Process Automation for Scalable Cloud Operations and Dynamic Resource Optimization. Journal of Computational Analysis and Applications (JoCAAA), 33(06), 4207–4221.

3. Secinaro, S., Calandra, D., Secinaro, A., Muthurangu, V., & Biancone, P. (2021). The role of artificial intelligence in healthcare: A structured literature review. BMC Medical Informatics and Decision Making, 21, Article 125.

4. Goel, A., Raut, G., Sharma, A., & Taneja, U. (2024). Artificial intelligence and sustainable business: A review. South Asian Journal of Business and Management Cases, 13(3), 340–365.

5. Mondeddula, S. R. (2024). Large Language Model-Based Financial Intelligence for Automated Compliance, Risk Analysis, and Regulatory Reporting. Journal of Computational Analysis and Applications (JoCAAA), 33(06), 4222–4227.

6. Crompton, H., & Burke, D. (2023). Artificial intelligence in higher education: The state of the field. International Journal of Educational Technology in Higher Education, 20, Article 22.

7. Charfeddine, L., & Umlai, M. (2023). ICT sector, digitization and environmental sustainability: A systematic review of the literature from 2000 to 2022. Renewable and Sustainable Energy Reviews, 184, Article 113482.

8. Gorle, R. (2024). Deep Learning Approaches for Threat Detection in Multi-Cloud Environments. Journal of Computational Analysis and Applications (JoCAAA), 33(07), 3857–3864.

9. Wang, S., Wang, F., Zhu, Z., Wang, J., Tran, T., & Du, Z. (2024). Artificial intelligence in education: A systematic literature review. Expert Systems with Applications, 252, Article 124167.

10. Sasidhar Reddy Mondeddula. (2022). AI-Driven Fraud Detection Using Ensemble Machine Learning for Secure Digital Banking Transactions. International Journal of Intelligent Systems and Applications in Engineering, 10(3s), 597–605.

11. Dhiman, R., Miteff, S., Wang, Y., Ma, S.-C., Amirikas, R., & Fabian, B. (2024). Artificial intelligence and sustainability—A review. Analytics, 3(1), 140–164.

12. de la Torre-López, J., Ramírez, A., & Romero, J. R. (2023). Artificial intelligence to automate the systematic review of scientific literature. Computing, 105, 2171–2194.

13. Penaka, B. (2024). Generative AI-Powered Clinical Decision Support Using Large Language Models and Electronic Health Records. Journal of Neonatal Surgery, 13(1), 2588–2596.

14. Stahl, B. C., Antoniou, J., Bhalla, N., Brooks, L., Jansen, P., Lindqvist, B., Kirichenko, A., Marchal, S., Rodrigues, R., Santiago, N., Warso, Z., & Wright, D. (2023). A systematic review of artificial intelligence impact assessments. Artificial Intelligence Review, 56, 12799–12831.

15. Ellenki, R. R. (2024). Deep Learning-Based Demand Intelligence for Dynamic Merchandise Planning and Allocation. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 7796–7802.

16. Yusuf, A., Pervin, N., Román-González, M., & Noor, N. M. (2024). Generative AI in education and research: A systematic mapping review. Review of Education, 12, Article e3489.

17. Movva, V. R. (2024). AI-Augmented DevOps for Large-Scale Retail Platforms: A Framework for Intelligent CI/CD, Automated Testing, and Deployment Optimization. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 7759–7765.

18. Blaizot, A., Veettil, S. K., Saidoung, P., Moreno-Garcia, C. F., Wiratunga, N., Aceves-Martins, M., Lai, N. M., & Chaiyakunapruk, N. (2022). Using artificial intelligence methods for systematic review in health sciences: A systematic review. Research Synthesis Methods, 13(3), 353–362.

19. Kour, R., Karim, R., Dersin, P., & Venkatesh, N. (2024). Cybersecurity for Industry 5.0: Trends and gaps. Frontiers in Computer Science, 6, Article 1434436.

20. Mahadevan, S. (2024). Empowering Manufacturing: Generative AI Revolutionizes ERP Application. International Journal of Innovative Science and Research Technology, 9, 593–595.

21. Celik, I., Dindar, M., Muukkonen, H., & Järvelä, S. (2022). The promises and challenges of artificial intelligence for teachers: A systematic review of research. TechTrends, 66, 616–630.

22. Rajan, A. A., & Vetriselvi, V. (2024). Systematic survey: Secure and privacy-preserving big data analytics in cloud. Journal of Computer Information Systems, 64(1), 136–156.

23. Loganathan, R., & Kolla, S. H. (2024). Harnessing generative AI for adaptive risk policy generation in multi-regulatory data center environments. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 15(3), 505–515.

24. Castillo-Martínez, I. M., Flores-Bueno, D., Gómez-Puente, S. M., & Vite-León, V. O. (2024). AI in higher education: A systematic literature review. Frontiers in Education, 9, Article 1391485.

25. Tripathi, S., Bachmann, N., Brunner, M., Rizk, Z., & Jodlbauer, H. (2024). Assessing the current landscape of AI and sustainability

literature: Identifying key trends, addressing gaps and challenges. Journal of Big Data, 11, Article 65.

26. Mashetty, S. (2024). Leveraging Deep Learning, Neural Networks, and Data Engineering for Intelligent Mortgage Loan Validation: A Data-Driven Approach to Automating Borrower Income, Employment, and Asset Verification (December 21, 2024).

27. Mustafa, M. Y., et al. (2024). A systematic review of literature reviews on artificial intelligence in education (AIED): A roadmap to a future research agenda. Smart Learning Environments, 11, Article 59.

28. Heeg, D. M., & Avraamidou, L. (2023). The use of artificial intelligence in school science: A systematic literature review. Educational Media International, 60(2), 125–150.

29. Thayyib, P. V., Mamilla, R., Khan, M., Fatima, H., Asim, M., Anwar, I., Shamsudheen, M. K., & Khan, M. A. (2023). State-of-the-art of artificial intelligence and big data analytics reviews in five different domains: A bibliometric summary. Sustainability, 15(5), Article 4026.

30. Mondeddula, S. R. (2022). Machine Learning-Based Credit Risk Assessment For Intelligent Lending and Default Prediction in Financial Services. Journal of International Crisis and Risk Communication Research, 5(1), 113–121.

31. Stojanov, A., & Daniel, B. K. (2024). A decade of research into the application of big data and analytics in higher education: A systematic review of the literature. Education and Information Technologies, 29, 5807–5831.

32. Mahadevan, S., Desani, N. R., Yadav, P. S., Joseph, T., & Malcom, A. (2024). FutureTech Innovations. Cari Journals USA LLC.

33. García-Martínez, I., Fernández-Batanero, J. M., Fernández-Cerero, J., & León, S. P. (2023). Analysing the impact of artificial intelligence and computational sciences on student performance: Systematic review and meta-analysis. Journal of New Approaches in Educational Research, 12, 171–197.

34. Gorle, R. (2023). Machine Learning-Based Access Risk Detection in Cloud Identity and Access Management Systems. Journal of International Crisis and Risk Communication Research, 241–252.

35. Khanna, N., Khan, Z., Koubaa, A., Khand, M. K., & Salleh, R. (2024). Global insights and the impact of generative AI-ChatGPT on multidisciplinary: A systematic review and bibliometric analysis. Connection Science, 36(1).

36. Dwivedi, Y. K., et al. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 57, 101994.

37. Mahadevan, S. (2024). Empowering Manufacturing: Generative AI Revolutionizes ERP Application. International Journal of Innovative Science and Research Technology, 9, 593–595.