ORIGINAL RESEARCH **Open access**

A Responsible AI Readiness Model for Energy Utilities: Organizational Capabilities, Data Governance, Risk Management, and Regulatory Alignment

Ursula Hoffmann[1*], Stefan Meier[1]

Abstract

Energy utilities are increasingly adopting artificial intelligence to support grid management, renewable integration, demand response, predictive maintenance, cybersecurity, and customer-facing operations. However, AI deployment in the utility sector carries responsibilities that extend beyond technical performance because algorithmic decisions can affect reliability, safety, affordability, equity, consumer trust, and regulatory accountability. Existing AI readiness models are often too generic to capture the distinctive obligations of utilities as operators of critical infrastructure and providers of essential public services. This article develops a responsible AI readiness model tailored to energy utilities through conceptual synthesis of responsible AI principles, organizational AI readiness literature, smart grid data governance, risk management, energy regulation, and utility management studies. The proposed model is structured around four interconnected dimensions: Organizational Capabilities, Data Governance, Risk Management, and Regulatory Alignment. Each dimension is interpreted through progressive readiness levels—Nascent, Developing, Mature, and Leading—to support qualitative diagnosis rather than numerical scoring. The model shows that responsible AI readiness depends not only on technical capability, but also on leadership accountability, workforce literacy, data quality, privacy protection, lifecycle risk controls, cybersecurity integration, vendor oversight, documentation, regulatory mapping, and consumer redress mechanisms. By translating broad responsible AI principles into sector-specific organizational capabilities, the model offers utilities, regulators, and governance bodies a practical framework for assessing institutional preparedness and guiding responsible AI deployment. The article contributes a conceptual readiness architecture for aligning AI innovation with public-interest obligations during the energy transition.

Keywords Responsible AI, Readiness model, Energy utilities, Organizational capabilities, AI risk management, Data governance

*Correspondence:
Ursula Hoffmann
ursula.hoffmann@ethz.ch
[1] Department of Artificial Intelligence for Smart Grid Optimization, Faculty of Electrical Engineering, ETH Zurich, Zurich, Switzerland

Introduction

Energy utilities are increasingly adopting artificial intelligence across smart metering, predictive maintenance, demand-side response, renewable forecasting, cybersecurity, and customer-facing operations. AI applications in sustainable energy and demand response demonstrate how data-driven systems can support operational flexibility, efficiency, and coordination under increasingly complex grid conditions [1]. Yet utilities differ from ordinary digital firms because they operate safety-critical infrastructure, deliver essential public services, and remain subject to intensive regulatory oversight. A responsible AI readiness model is therefore needed to reflect not only technological capability but also reliability, accountability, and public-interest obligations.

This is an open access article distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0), which permits non-commercial use, distribution, reproduction, and adaptation in any medium or format, provided that appropriate credit is given to the original author(s) and source, a link to the license is provided, and any changes made are indicated. Adapted material must be distributed under the same license.

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

The movement from isolated AI pilots to enterprise-wide deployment exposes organizational weaknesses that are often hidden during experimentation. Organizational AI readiness research suggests that firms require strategic alignment, data infrastructure, governance capacity, and managerial commitment before AI can create durable value [2]. Utility digitalization intensifies this challenge because decarbonization, decentralization, and digitalization are jointly reshaping power infrastructures and the organizations that manage them [3]. Without structured readiness, utilities may procure AI tools faster than they develop the internal capabilities needed to use them responsibly.

Responsible AI readiness can be conceptualized as an organization's capacity to deploy AI in ways that are technically robust, ethically defensible, operationally accountable, and legally aligned. Existing AI ethics and responsible AI work emphasizes principles such as fairness, transparency, accountability, privacy, robustness, and human oversight, but these principles require organizational translation before they can affect practice [4]. Readiness models can help bridge this gap by converting broad principles into assessable capability areas, decision routines, and governance expectations. For utilities, such a model must also account for grid reliability, consumer vulnerability, energy justice, and regulated service provision.

This article proposes a responsible AI readiness model specifically designed for energy utilities and structured around Organizational Capabilities, Data Governance, Risk Management, and Regulatory Alignment. The model draws from organizational AI capability literature, responsible AI frameworks, smart grid data governance, cybersecurity, energy justice, and regulatory analysis [5]. Its intended use is conceptual and diagnostic: it can support internal reflection, executive planning, governance design, and regulator–utility dialogue, but it is not presented as an empirically validated measurement instrument. The contribution is a sector-specific readiness architecture that connects AI adoption with the distinctive public obligations of energy utilities.

Background

AI in the energy utility sector: from automation to autonomous decisions

AI in energy utilities has expanded from conventional automation toward systems that classify, predict, recommend, and sometimes trigger operational responses. Applications now include demand-side response, smart grid analytics, peer-to-peer energy trading, distributed energy coordination, predictive maintenance, cybersecurity detection, and customer segmentation [6]. Peer-to-peer and community-based market research shows that digital platforms increasingly mediate transactions among distributed actors, creating more complex decision environments for utilities and regulators [7]. As these systems become more autonomous, readiness must include organizational ability to supervise AI-mediated decisions rather than merely install digital tools.

Responsible AI principles and their relevance to utilities

Responsible AI principles carry special weight in the utility sector because decisions can affect energy access, billing, reliability, demand response participation, and exposure to service disruption. The global landscape of AI ethics guidelines identifies recurring commitments to transparency, justice, responsibility, privacy, and non-maleficence, but these commitments remain abstract unless embedded in organizational processes [4]. Work on AI ethics implementation similarly shows that principles require tools, methods, and accountable practices to become operational [8]. For utilities, responsible AI should therefore be understood as an infrastructure governance concern rather than a narrow technical compliance exercise.

Organizational readiness and maturity models for AI

AI readiness and maturity models usually emphasize leadership support, technical skills, data resources, strategic alignment, and change capacity. Research on organizational AI readiness identifies the importance of value creation, data, governance, people, and organizational culture as readiness factors [2]. AI capability research similarly frames AI as

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

a composite organizational capability that combines tangible resources, human skills, and intangible governance assets [5]. However, generic readiness models are limited for energy utilities because they rarely address regulated monopoly functions, service obligations, grid reliability, consumer protection, or critical infrastructure risk.

Data governance in the energy context

Energy utilities manage unusually sensitive and operationally consequential data, including smart meter readings, grid telemetry, asset records, outage histories, customer profiles, and increasingly granular consumption patterns. Smart meter privacy research shows that energy data can reveal behavioral patterns, household routines, and occupancy signals, making privacy governance central to responsible AI [9]. Big data analytics in smart grids also depends on data quality, integration, timeliness, and interoperability across heterogeneous systems [10]. Responsible AI readiness in utilities must therefore treat data governance as a strategic capability rather than an information technology support function.

AI risk management and regulatory compliance for critical infrastructure

AI risk management in energy utilities must address technical failure, cyber vulnerability, algorithmic bias, unsafe automation, regulatory breach, and consumer harm. Smart grid cybersecurity research shows that digitalization introduces attack surfaces across communication networks, meters, control systems, and distributed assets [11]. Regulatory analysis of the EU Artificial Intelligence Act demonstrates that AI governance is increasingly moving from voluntary ethics toward risk-based legal obligations [12]. Although broader frameworks such as AI risk management standards are not cited here as primary references, the literature indicates that utilities will need internal risk processes capable of translating emerging AI regulation into operational controls.

Recent scholarship further emphasizes that responsible AI governance in energy systems depends on explainability, institutional accountability, and operational transparency across AI-enabled grid infrastructures. Reviews of AI governance in smart energy systems show that explainability, fairness, accountability, and stakeholder trust are becoming central governance requirements for utilities deploying AI in critical infrastructure environments [13]. Emerging regulatory analyses also indicate that energy-sector AI governance is shifting toward more formalized compliance expectations, especially in relation to transparency obligations, risk-based oversight, and sector-specific governance mechanisms [14]. These developments reinforce the importance of sector-specific readiness models capable of integrating organizational governance with evolving legal and technical requirements.

Conceptual Foundation of the Readiness Model

Defining responsible AI readiness for energy utilities

Responsible AI readiness for energy utilities can be defined as a multi-dimensional organizational capacity to design, procure, deploy, monitor, and govern AI systems in ways that are safe, ethical, reliable, transparent, and legally aligned. This capacity includes technical foundations, managerial structures, data governance, risk control, stakeholder accountability, and regulatory intelligence. Literature on AI business value suggests that organizations derive value from AI only when technology is integrated with process, governance, and organizational transformation [15]. Readiness is therefore dynamic and learnable rather than a binary state that a utility either possesses or lacks.

Dimensions as interconnected capability areas

The model treats Organizational Capabilities, Data Governance, Risk Management, and Regulatory Alignment as interconnected capability areas rather than independent modules. Strategic AI capability can be weakened if data quality is poor, risk ownership is unclear, or compliance processes are detached from operational decision-making [16]. Similarly, responsible AI principles cannot be translated into practice if workforce literacy, documentation, and escalation channels

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

are underdeveloped [8]. In energy utilities, weakness in one dimension can propagate across others because operational decisions, customer impacts, grid reliability, and regulatory accountability are tightly coupled.

Readiness levels as developmental stages

Readiness levels can be conceptualized as developmental stages that describe qualitatively different configurations of practice, culture, and governance. A nascent utility may rely on fragmented AI pilots, while a developing utility begins to standardize review processes and assign accountability. A mature utility integrates AI governance into enterprise risk, data management, compliance, and operational monitoring, while a leading utility actively shapes regulatory practice and responsible innovation ecosystems. This staged logic is consistent with maturity-oriented thinking in digital transformation, but it requires sector-specific adaptation to avoid treating all AI adoption as equivalent [17].

The proposed model organizes responsible AI readiness into four interconnected capability areas: Organizational Capabilities, Data Governance, Risk Management, and Regulatory Alignment. These dimensions are interpreted developmentally across four readiness levels: Nascent, Developing, Mature, and Leading, as shown in **Figure 1.**

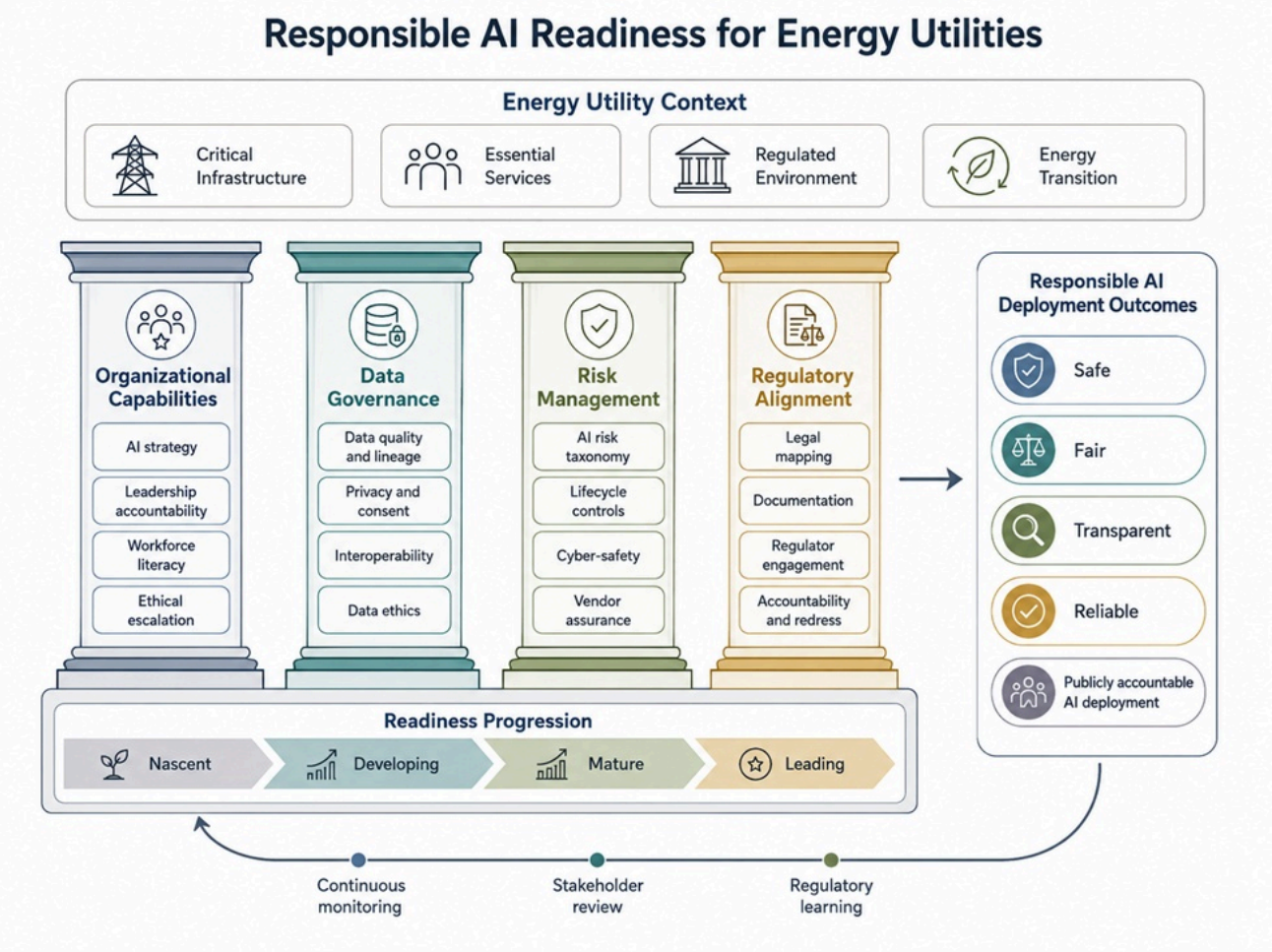


Figure 1. Responsible AI readiness model for energy utilities.

Model Dimensions and Readiness Levels

Organizational capabilities

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

Organizational Capabilities refer to the leadership, skills, structures, culture, and coordination mechanisms that allow a utility to adopt AI responsibly. Responsible AI readiness would typically include executive sponsorship, a clearly articulated AI strategy, cross-functional collaboration, workforce development, and escalation pathways for ethical concerns. Studies of AI-enabled organizations emphasize that AI capability depends not only on technical resources but also on managerial commitment, learning culture, and organizational alignment [5]. In utilities, these capabilities must be tied to public value, service reliability, and the institutional obligation to act prudently on behalf of customers.

Data governance

Data Governance concerns the rules, processes, and responsibilities through which utilities ensure that data used for AI is accurate, secure, privacy-preserving, interoperable, and ethically appropriate. Smart grid data governance must cover smart meters, supervisory control systems, customer information systems, geographic data, market data, and third-party data flows. Smart meter privacy research indicates that consumption data requires special protection because it may reveal intimate household behaviors [9]. At the same time, smart grid analytics depends on integrated and high-quality data pipelines, making data governance central to both AI performance and accountability [10].

Risk management

Risk Management refers to the capacity to identify, assess, mitigate, monitor, and respond to AI-related harms across the AI lifecycle. In energy utilities, this includes operational safety risks, grid reliability risks, bias in customer-facing decisions, cybersecurity threats, vendor dependencies, reputational harms, and regulatory sanctions. Cybersecurity studies show that smart grids face complex threats across communication, sensing, and control layers, which makes AI risk inseparable from broader digital infrastructure risk [11]. As shown in **Table 1**, the model translates these dimensions into sub-dimensions and indicative readiness levels that utilities could use for structured self-assessment.

Table 1. AI Governance Readiness Framework for Energy Utilities: Organizational Capabilities, Data Governance, Risk Management, and Regulatory Alignment

Dimension	Sub-Dimensions	Nascent	Developing	Mature	Leading
Organizational Capabilities	AI strategy and public-value alignment	Isolated project logic	Strategy draft linked to business cases	Portfolio aligned with reliability and equity goals	AI strategy embedded in public-interest performance governance
Organizational Capabilities	Leadership accountability and role clarity	Informal executive interest	Named sponsor for selected AI initiatives	Accountable senior owner and documented decision rights	Board-level AI accountability with transparent mandate
Organizational Capabilities	Workforce literacy and hybrid expertise	Specialist-dependent knowledge	Basic awareness training for selected teams	Cross-functional AI literacy across technical and customer units	Utility-wide responsible AI competency pathways
Organizational Capabilities	Ethical culture and escalation	Concerns handled ad hoc	Early issue-reporting channels	Formal challenge, review, and escalation routines	Protected contestation culture with learning loops

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

Data Governance	Data quality and lineage	Unmapped source systems	Partial inventories and manual checks	Traceable data pipelines with quality controls	Proactive lineage assurance across AI-critical datasets
Data Governance	Privacy and consent management	Compliance treated as legal afterthought	Consent and privacy checks added during projects	Privacy-by-design embedded in AI lifecycle	Consumer data stewardship treated as strategic trust asset
Data Governance	Interoperability and data sharing	Fragmented local formats	Bilateral sharing agreements	Standardized data access and integration protocols	Secure ecosystem-level interoperability with accountability clauses
Data Governance	Data ethics and representativeness	Bias concerns recognized late	Basic representativeness checks	Documented fairness-sensitive data review	Continuous equity-aware data stewardship
Risk Management	AI risk taxonomy and ownership	Undefined AI risk categories	Preliminary AI risk register	Enterprise AI risk taxonomy with owners	Sector-specific risk ontology aligned with resilience planning
Risk Management	Mitigation and monitoring controls	Manual post-deployment fixes	Limited pre-release checks	Lifecycle controls for testing, monitoring, and response	Adaptive monitoring with independent assurance
Risk Management	Cybersecurity and operational safety	Security review separated from AI work	AI security considered for major systems	Integrated cyber-safety review for AI deployment	AI, cyber, and grid resilience jointly governed
Risk Management	Third-party and vendor risk	Procurement based on functionality	Basic vendor questionnaires	Responsible AI clauses in procurement and audit rights	Supplier ecosystem governed through shared assurance standards
Regulatory Alignment	Legal awareness and compliance mapping	Reactive legal interpretation	Project-level regulatory screening	Systematic mapping of AI use cases to obligations	Anticipatory compliance integrated into strategic planning
Regulatory Alignment	Documentation and reporting	Minimal model documentation	Basic records for high-risk use cases	Standardized documentation for audit and review	Transparent reporting aligned with regulator and stakeholder needs
Regulatory Alignment	Regulator engagement	Contact only during approval or dispute	Occasional consultation	Structured dialogue with	Active participation in regulatory

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

				regulators and consumer bodies	learning and sandbox design
Regulatory Alignment	Accountability and redress	Unclear complaint pathways	Existing customer processes adapted	AI-specific accountability and appeal channels	Contestability embedded in service design and oversight

Organizational Capabilities for Responsible AI

Leadership, strategy, and ethical culture

Responsible AI readiness begins with leadership commitment that frames AI as a governed organizational capability rather than a collection of technical experiments. Work on organizing in the age of learning algorithms shows that algorithmic systems reshape roles, authority, and coordination, requiring organizations to reconsider how accountability is distributed [18]. In utilities, leadership should connect AI strategy to reliability, affordability, decarbonization, customer protection, and public trust. Ethical culture should be characterized by the ability of employees to question automated recommendations, escalate concerns, and pause deployment when risks exceed organizational tolerance.

Workforce development and AI literacy

Responsible AI readiness also depends on workforce development that equips engineers, operators, customer service teams, compliance staff, and executives to understand AI capabilities and limitations. AI capability research indicates that human skills and organizational knowledge are central to realizing value from AI, not merely complements to software investment [5]. Utilities need hybrid roles that combine power systems knowledge, data science, cybersecurity awareness, customer protection, and responsible AI judgment. Such literacy could be assessed through training coverage, role-specific competencies, scenario-based exercises, and evidence that staff can interpret and challenge AI outputs.

Cross-functional governance and responsible AI roles

Cross-functional governance is needed because AI decisions in utilities often cut across information technology, operations, legal, regulatory affairs, customer service, cybersecurity, and executive risk oversight. The literature on translating AI ethics into practice emphasizes that responsible AI requires tools, role allocation, and organizational methods rather than principle statements alone [8]. Utilities could establish AI ethics committees, responsible AI officers, model review boards, or cross-functional approval gates for high-impact systems. These structures should not create symbolic compliance only; they should have authority to demand documentation, request redesign, impose conditions, and escalate unresolved risks.

Data Governance and AI Lifecycle Management

Data quality, lineage, and bias prevention

Utilities must govern data from smart meters, SCADA systems, outage management systems, asset registries, geographic information systems, customer accounts, and market platforms. Smart grid analytics research shows that data volume, velocity, heterogeneity, and quality are central barriers to extracting reliable value from grid data [10]. Bias prevention requires attention to missingness, measurement error, uneven deployment of sensors, historical service disparities, and underrepresentation of vulnerable customers. Readiness could be assessed through data lineage documentation, quality thresholds, bias-sensitive preprocessing, and clear ownership for AI-critical datasets.

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

Data privacy, security, and consumer consent

Responsible AI in utilities must manage the tension between data-intensive optimization and the privacy rights of energy consumers. Smart meter privacy literature shows that granular consumption records can disclose occupancy, habits, and appliance use, making privacy-preserving governance essential [9]. Security research on smart grid metering networks further shows that privacy cannot be separated from authentication, communication security, and resilience against malicious access [19]. Utilities should therefore treat consumer consent, data minimization, encryption, access controls, and privacy-preserving analytics as readiness indicators rather than peripheral compliance tasks.

Data sharing and interoperability governance

AI-enabled utility operations increasingly require data sharing among distribution system operators, aggregators, retailers, transmission operators, regulators, technology vendors, and community energy actors. Blockchain and peer-to-peer energy research highlights both the potential and complexity of decentralized energy data exchange, where trust, governance, and technical interoperability become central concerns [20]. Community-based energy market studies likewise show that data-sharing arrangements shape participation, accountability, and coordination across actors [7]. Readiness in this area should be characterized by interoperable standards, contractual safeguards, auditable data access, and mechanisms that protect customer rights while enabling system coordination.

Data ethics and algorithmic transparency

Data governance for responsible AI must extend beyond technical quality and privacy to include ethical use, representativeness, and transparency. Energy justice research on smart grids shows that digital energy systems can reproduce inequities if social vulnerability, participation, and procedural fairness are insufficiently considered [21]. In utility AI, data ethics should address whether training data reflect diverse customer groups, whether proxies create discriminatory effects, and whether consumers can understand how their data affect decisions. Algorithmic transparency would typically include data-use notices, model documentation, explanation channels, and internal records that connect data sources to decision consequences.

Risk Management and Ethical Safeguards

AI-specific risk taxonomies for energy utilities

An AI-specific risk taxonomy for utilities should cover operational safety, grid reliability, cybersecurity, consumer harm, algorithmic bias, reputational damage, vendor opacity, and regulatory sanction. Research on smart grid resilience shows that modern grids must be evaluated not only for efficiency but also for their capacity to withstand, adapt to, and recover from disruptions [22]. Machine learning for smart grid cybersecurity further indicates that AI can be both a defensive tool and a source of new vulnerabilities when embedded in complex infrastructure [23]. A utility readiness model should therefore classify risks according to affected function, harm pathway, affected stakeholder, and required control mechanism. **Figure 2** illustrates an AI-specific utility risk taxonomy framed as an integrated lifecycle model, showing how risks in energy utilities emerge through affected functions, harm pathways, stakeholders, and control mechanisms across design, procurement, deployment, monitoring, and retirement.

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

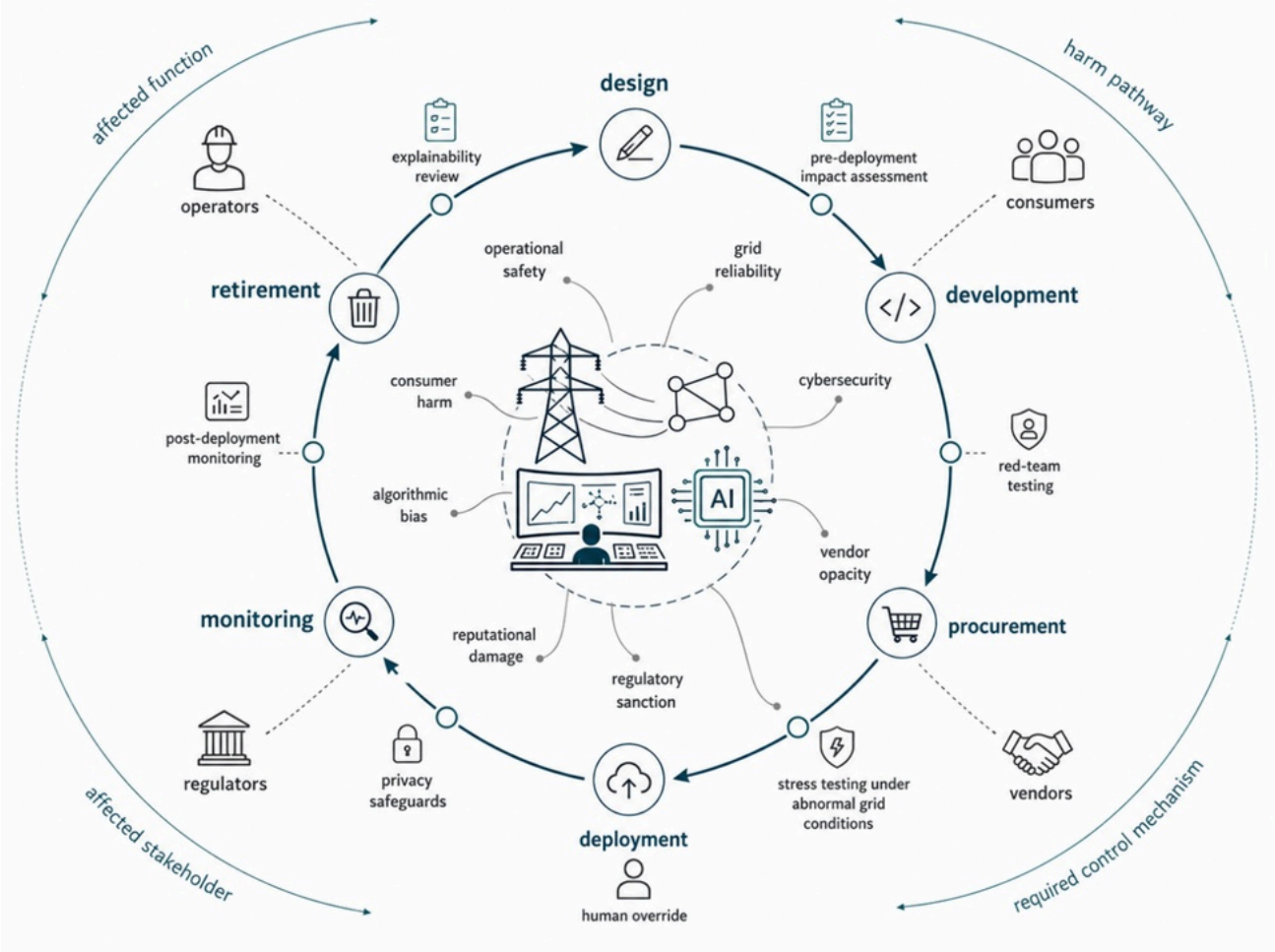


Figure 2. Lifecycle-Oriented AI Risk Taxonomy for Energy Utilities

Risk assessment and mitigation across the AI lifecycle

AI risks should be assessed across design, development, procurement, deployment, monitoring, and retirement rather than only at the point of technical testing. Systematic reviews of AI impact assessments show that structured assessment can support anticipation of ethical, social, legal, and technical impacts before harm occurs [24]. Trustworthy AI literature similarly emphasizes robustness, accountability, explainability, privacy, and human control as recurring requirements for responsible deployment [25]. In utilities, lifecycle risk mitigation could include pre-deployment impact assessment, red-team exercises, stress testing under abnormal grid conditions, human override design, and post-deployment review.

Continuous monitoring and incident response

Continuous monitoring is essential because deployed AI systems can drift as grid conditions, customer behavior, weather patterns, market rules, and technology environments change. AI ethics critiques warn that ethical principles can become ineffective unless they are connected to concrete accountability and enforcement mechanisms [26]. Utility AI systems should therefore be monitored for performance degradation, bias emergence, cybersecurity anomalies, unsafe recommendations, and unexplained changes in decision behavior. Incident response protocols should specify thresholds for intervention, responsible teams, communication duties, consumer remedies, and conditions under which systems must be suspended.

Third-party and supply chain AI risk

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

Energy utilities increasingly rely on vendor platforms, cloud services, external analytics providers, and embedded AI within operational technology. This creates supply chain risk because utilities may depend on models they did not design, data pipelines they do not fully control, and proprietary systems that limit explainability. Reviews of trustworthy AI show that accountability, transparency, and robustness are difficult to assure when system boundaries and responsibilities are unclear [25]. Responsible AI procurement should therefore include vendor documentation requirements, audit rights, data-use restrictions, cybersecurity obligations, explainability expectations, and exit strategies for high-risk AI services.

Regulatory Alignment and Governance Integration

Mapping AI regulations to utility operations

Regulatory alignment requires utilities to map emerging AI obligations onto existing energy regulation, consumer protection, cybersecurity rules, market oversight, and grid reliability requirements. Analysis of the Draft EU Artificial Intelligence Act shows that risk-based AI regulation can create obligations related to documentation, human oversight, transparency, risk management, and conformity assessment [12]. Responsible AI frameworks that connect principles to regulation indicate that organizations must translate abstract requirements into system-specific governance practices [27]. For utilities, this means identifying which AI use cases affect safety, access, billing, demand response, outage management, or vulnerable consumers and then aligning controls accordingly.

Embedding readiness into corporate governance

Responsible AI readiness should be embedded into existing corporate governance mechanisms rather than managed as a temporary innovation initiative. AI ethics research across public, private, and civil society sectors shows that accountability depends on institutional ownership, documentation, and oversight arrangements [28]. In utilities, board oversight, audit committees, enterprise risk management, regulatory affairs, compliance functions, and annual reporting can all be used to sustain attention to responsible AI. **Figure 3** illustrates how responsible AI readiness in utilities depends on translating external AI obligations into operational controls and embedding those controls within durable corporate governance mechanisms.

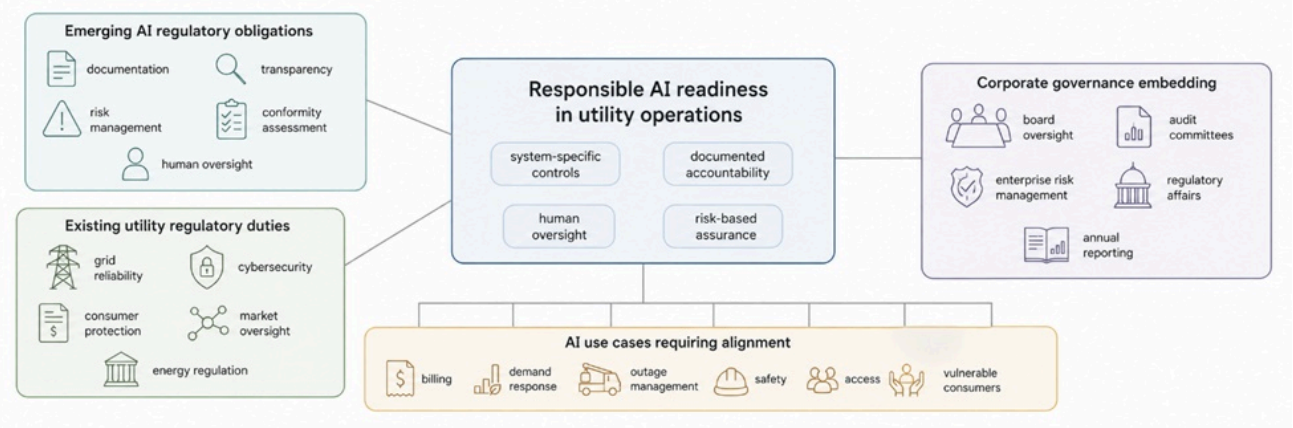


Figure 3. Regulatory Alignment and Corporate Governance Embedding for Responsible AI Readiness in Utilities

Table 2 maps the readiness dimensions to governance mechanisms and regulatory instruments that could support practical operationalization.

Table 2. Governance Mechanisms and Regulatory Instruments Supporting Responsible AI Readiness in Energy Utilities

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

Model Dimension	Governance Mechanisms	Regulatory Instruments
Organizational Capabilities	Board AI oversight charter; executive responsible AI sponsor; cross-functional AI review board; role-based AI literacy program; protected escalation pathway for AI concerns	Corporate governance codes; regulated utility performance obligations; workforce competence expectations; consumer-duty principles; public-interest reporting requirements
Data Governance	AI-critical data inventory; data lineage registry; privacy-by-design checklist; smart meter data access controls; third-party data-sharing approval workflow	Data protection law; smart meter privacy rules; grid data access codes; interoperability standards; consumer consent and disclosure requirements
Risk Management	AI risk register; lifecycle impact assessment; cyber-safety review gate; incident response playbook; vendor assurance questionnaire; independent model review	AI risk management frameworks; cybersecurity regulation; critical infrastructure protection rules; audit and assurance requirements; procurement compliance clauses
Regulatory Alignment	AI use-case classification map; legal obligation tracker; regulator engagement protocol; documentation repository; compliance evidence dashboard	EU-style risk-based AI regulation; energy regulator guidance; transparency duties; regulatory sandbox procedures; conformity assessment and reporting obligations
Integrated Utility Governance	Enterprise responsible AI committee; audit committee reporting line; annual responsible AI statement; consumer appeal and redress workflow; joint AI–cyber–reliability review	Annual regulatory filings; service-quality standards; consumer protection rules; reliability performance frameworks; public accountability and consultation processes

Evaluation Strategy for the Readiness Model

Conceptual validity and domain appropriateness

The model's conceptual validity could be evaluated by examining whether its dimensions adequately reflect responsible AI principles, organizational AI readiness theory, and the operational realities of energy utilities. Connecting the dots between AI principles, ethics, requirements, and regulation suggests that responsible AI systems require coherent links between values, governance processes, and technical controls [27]. Domain appropriateness would require assessing whether the model captures the special features of utilities, including critical infrastructure, regulated service provision, smart grid data, and consumer vulnerability. The model should therefore be judged not by numerical precision at this stage but by coherence, relevance, completeness, and explanatory usefulness.

Table 3 summarizes potential indicators that utilities may use to qualitatively evaluate responsible AI readiness across the four dimensions of the proposed model.

Table 3. Illustrative Qualitative Indicators for Evaluating Responsible AI Readiness in Energy Utilities

Model Dimension	Illustrative Evaluation Indicators	Example Evidence Sources
Organizational Capabilities	Executive AI governance ownership; workforce AI literacy; cross-functional coordination; ethical escalation mechanisms	AI strategy documents; governance charters; staff training records; committee reports

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

Data Governance	Data lineage transparency; privacy-by-design practices; interoperability standards; fairness-sensitive data review	Data inventories; privacy audits; interoperability protocols; model documentation
Risk Management	AI lifecycle risk assessment; cybersecurity integration; incident response readiness; vendor assurance controls	Risk registers; cyber review reports; incident response plans; procurement contracts
Regulatory Alignment	AI compliance mapping; regulator engagement practices; audit readiness; consumer accountability mechanisms	Compliance matrices; regulatory submissions; audit logs; customer appeal procedures

Utility stakeholder validation through expert review

Future validation could involve expert panels, Delphi studies, scenario workshops, or structured review by utility executives, engineers, regulators, consumer advocates, cybersecurity specialists, and data governance professionals. Renewable energy community research shows that governance models in energy systems must account for institutional design, stakeholder participation, and changing roles within decentralized systems [29]. Stakeholder review would help determine whether the readiness levels are understandable, whether sub-dimensions reflect real utility practices, and whether governance mechanisms are feasible across different organizational contexts. Such validation should be conducted before converting the model into any formal assessment instrument.

Applicability across utility types and regions

The model is intended to be adaptable across vertically integrated utilities, distribution network operators, transmission system operators, retailers, municipal utilities, and community-oriented energy organizations. Peer-to-peer trading research shows that electricity networks are becoming more actor-rich and transactionally complex, creating different governance needs across market structures [30]. Regional transferability would also depend on differences in energy law, data protection, market liberalization, customer rights, and regulatory capacity. The model therefore provides a conceptual architecture rather than a universal checklist, and its use in specific jurisdictions would require contextual interpretation.

Limitations

The model as a conceptual artefact requiring empirical grounding

The proposed model is a conceptual artefact and does not report empirical testing, maturity scores, survey results, or statistical validation. This limitation is important because constructs such as ethical culture, accountable governance, and responsible innovation are difficult to operationalize without stakeholder interpretation and contextual evidence. AI impact assessment literature suggests that assessment tools require careful design, validation, and institutional fit before they can support reliable decision-making [24]. Future research should therefore translate the model into indicators, test its usability, and examine whether it supports better governance outcomes in real utility settings.

The dynamic nature of AI technology and regulation

A second limitation is that AI technologies, regulatory expectations, cybersecurity threats, and utility business models are changing rapidly. Reviews of artificial intelligence in sustainable energy show that the field continues to evolve across applications, methods, and governance challenges [1]. As AI becomes embedded in distributed energy resources, customer platforms, grid-edge devices, and automated markets, the readiness model may require periodic revision. The model should therefore be treated as an adaptive governance architecture rather than a fixed standard.

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

Conclusion

The responsible AI readiness model proposed in this article offers a structured way for energy utilities to move from fragmented AI experimentation toward systematic and accountable deployment. Its four dimensions—Organizational Capabilities, Data Governance, Risk Management, and Regulatory Alignment—capture the main capability areas that utilities must develop to govern AI responsibly. The model is assessment-oriented but conceptual, meaning that it supports reflection, planning, and dialogue rather than numerical scoring. It provides a way to describe readiness as a developmental condition that can improve through deliberate governance action.

The utility sector carries responsibilities that make generic AI readiness approaches insufficient. Energy utilities operate critical infrastructure, provide essential services, manage sensitive consumer data, and act within dense regulatory environments. AI systems in this sector can affect reliability, equity, affordability, safety, and public confidence. A readiness model for utilities must therefore integrate technical competence with institutional accountability and public-interest reasoning.

The readiness levels and governance mapping tables add practical value by translating broad responsible AI concerns into assessable organizational patterns. **Table 1** supports internal diagnosis by showing how readiness may differ across dimensions and developmental stages. **Table 2** supports governance integration by connecting model dimensions to mechanisms that executives, boards, regulators, and compliance teams can recognize. Together, these tools can support more productive conversations between utilities and regulators about what responsible AI deployment should require in practice.

Future work should refine, validate, and operationalize the model through collaboration among utilities, regulators, consumer representatives, engineers, data scientists, and responsible AI scholars. Empirical validation will be necessary before the model can become a formal assessment instrument. Cross-sector learning from critical infrastructure, public administration, cybersecurity, and energy governance can strengthen its applicability. Ultimately, responsible AI readiness should become part of how utilities are evaluated, governed, and trusted during the energy transition.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 30 Aug 2022 Revised: 04 Nov 2022 Accepted: 21 Nov 2022
Published online: 15 November 2023

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at https://creativecommons.org/licenses/by-nc-sa/4.0/.

References

1. Ahmad T, Zhang D, Huang C, Zhang H, Dai N, Song Y, et al. Artificial intelligence in sustainable energy industry: Status quo, challenges and opportunities. J Clean Prod. 2021;289:125834.

2. Jöhnk J, Weißert M, Wyrtki K. Ready or not, AI comes—An interview study of organizational AI readiness factors. Bus Inf Syst Eng. 2021;63(1):5-20.

3. Di Silvestre ML, Favuzza S, Sanseverino ER, Zizzo G. How decarbonization, digitalization and decentralization are changing key power infrastructures. Renew Sustain Energy Rev. 2018;93:483-98.

4. Jobin A, Ienca M, Vayena E. The global landscape of AI ethics guidelines. Nat Mach Intell. 2019;1(9):389-99.

5. Mikalef P, Gupta M. Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. Inf Manag. 2021;58(3):103434.

6. Antonopoulos I, Robu V, Couraud B, Kirli D, Norbu S, Kiprakis A, et al. Artificial intelligence and machine learning approaches to energy demand-side response: A systematic review. Renew Sustain Energy Rev. 2020;130:109899.

7. Sousa T, Soares T, Pinson P, Moret F, Baroche T, Sorin E. Peer-to-peer and community-based markets: A comprehensive review. Renew Sustain Energy Rev. 2019;104:367-78.

8. Morley J, Floridi L, Kinsey L, Elhalal A. From what to how: An initial review of publicly available AI ethics tools, methods and research to translate principles into practices. In: Ethics, governance, and policies in artificial intelligence. Cham: Springer International Publishing; 2021. p. 153-183.

9. Asghar MR, Dán G, Miorandi D, Chlamtac I. Smart meter data privacy: A survey. IEEE Commun Surv Tutor. 2017;19(4):2820-35.

10. Bhattarai BP, Paudyal S, Luo Y, Mohanpurkar M, Cheung K, Tonkoski R, et al. Big data analytics in smart grids: State-of-the-art, challenges, opportunities, and future directions. IET Smart Grid. 2019;2(2):141-54.

11. Gunduz MZ, Das R. Cyber-security on smart grid: Threats and potential solutions. Comput Netw. 2020;169:107094.

12. Veale M, Borgesius FZ. Demystifying the draft EU artificial intelligence act. arXiv. 2021. arXiv:2107.03721.

13. Alsaigh R, Mehmood R, Katib I. AI explainability and governance in smart energy systems: A review. Front Energy Res. 2023;11:1071291.

14. Metaxas A. On the way to EU's clean energy transition: New approaches and challenges for gas regulation in the EU. J World Energy Law Bus. 2024;17(1):69-86.

15. Enholm IM, Papagiannidis E, Mikalef P, Krogstie J. Artificial intelligence and business value: A literature review. Inf Syst Front. 2022;24(5):1709-34.

16. Borges AF, Laurindo FJ, Spínola MM, Gonçalves RF, Mattos CA. The strategic use of artificial intelligence in the digital era: Systematic literature review and future research directions. Int J Inf Manage. 2021;57:102225.

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press

17. Brock JK, von Wangenheim F. Demystifying AI: What digital transformation leaders can teach you about realistic artificial intelligence. Calif Manage Rev. 2019;61(4):110-34.

18. Faraj S, Pachidi S, Sayegh K. Working and organizing in the age of the learning algorithm. Inf Organ. 2018;28(1):62-70.

19. Kumar P, Lin Y, Bai G, Paverd A, Dong JS, Martin A. Smart grid metering networks: A survey on security, privacy and open research issues. IEEE Commun Surv Tutor. 2019;21(3):2886-927.

20. Andoni M, Robu V, Flynn D, Abram S, Geach D, Jenkins D, et al. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew Sustain Energy Rev. 2019;100:143-74.

21. Milchram C, Hillerbrand R, van de Kaa G, Doorn N, Künneke R. Energy justice and smart grid systems: Evidence from the Netherlands and the United Kingdom. Appl Energy. 2018;229:1244-59.

22. Das L, Munikoti S, Natarajan B, Srinivasan B. Measuring smart grid resilience: Methods, challenges and opportunities. Renew Sustain Energy Rev. 2020;130:109918.

23. Berghout T, Benbouzid M, Muyeen SM. Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. Int J Crit Infrastruct Prot. 2022;38:100547.

24. Stahl BC, Antoniou J, Bhalla N, Brooks L, Jansen P, Lindqvist B, et al. A systematic review of artificial intelligence impact assessments. Artif Intell Rev. 2023;56(11):12799-831.

25. Kaur D, Uslu S, Rittichier KJ, Durresi A. Trustworthy artificial intelligence: A review. ACM Comput Surv. 2022;55(2):1-38.

26. Munn L. The uselessness of AI ethics. AI Ethics. 2023;3(3):869-77.

27. Díaz-Rodríguez N, Del Ser J, Coeckelbergh M, De Prado ML, Herrera-Viedma E, Herrera F. Connecting the dots in trustworthy artificial intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. Inf Fusion. 2023;99:101896.

28. Schiff D, Borenstein J, Biddle J, Laas K. AI ethics in the public, private, and NGO sectors: A review of a global document collection. IEEE Trans Technol Soc. 2021;2(1):31-42.

29. Lowitzsch J, Hoicka CE, van Tulder FJ. Renewable energy communities under the 2019 European Clean Energy Package—Governance model for the energy clusters of the future? Renew Sustain Energy Rev. 2020;122:109489.

30. Tushar W, Saha TK, Yuen C, Smith D, Poor HV. Peer-to-peer trading in electricity networks: An overview. IEEE Trans Smart Grid. 2020;11(4):3185-200.

© 2023 The Author(s). | Published by Institute of Smart Energy Systems Press