

ORIGINAL RESEARCH

Open access

AI Liability in Precision Agriculture: An Accountability Framework Across Data, Model, Platform, Advisory, and Machinery Layers

Ivan Georgiev¹, Elena Petrova^{1*}, Nikolay Stoyanov², Petar Kolev³

Abstract

Artificial intelligence is becoming embedded in precision agriculture through data-intensive monitoring, predictive models, digital platforms, advisory systems, robotics, and automated machinery. These arrangements complicate accountability because consequential outputs may result from interactions among data providers, model developers, platform operators, advisors, machinery manufacturers, system integrators, service providers, and farm operators rather than from a single actor or technical component. This article proposes a conceptual accountability framework for examining AI liability issues across agricultural AI systems without treating accountability mapping as a substitute for legal interpretation. The framework begins with agricultural use-case definition and stakeholder-role mapping, then examines data-level duties concerning quality, provenance, access, control, privacy, cybersecurity, and governance. It further maps model-level responsibilities for documentation, validation, robustness, bias assessment, explainability, uncertainty communication, and drift monitoring. Platform and advisory layers are addressed through governance, interface design, monitoring, escalation, human review, professional interpretation, and farmer-autonomy requirements. Machinery, automation, and operational risks are incorporated through control-system responsibilities, sensor-to-actuator traceability, supervisory control, fail-safe design, maintenance, incident reporting, and operational boundaries. The framework also identifies liability gaps created by fragmented evidence, unclear validation ownership, platform ambiguity, ineffective human oversight, and incomplete traceability. Its contribution is a structured method for clarifying responsibility pathways, evidence needs, decision boundaries, and governance gaps across interconnected agricultural AI layers. The framework is conceptual and does not determine legal liability, establish compliance, certify safety, allocate blame, or demonstrate deployment readiness.

Keywords Precision agriculture, Responsible AI, Accountability, Data governance, AI liability, Platform responsibility

*Correspondence:

Elena Petrova
elena.petrova@uni-sofia.bg

¹ Department of AI Liability and Agricultural Accountability, Faculty of Agriculture, Sofia University, Sofia, Bulgaria

² Department of Platform and Advisory Accountability, Faculty of Agriculture, University of Plovdiv, Plovdiv, Bulgaria

³ Department of Machinery and Model Liability, Faculty of Agriculture, University of Ruse, Ruse, Bulgaria

Introduction

Artificial intelligence in precision agriculture should be understood as part of a wider sociotechnical arrangement that connects farm data, analytical models, digital platforms, agricultural knowledge systems, machinery, and institutional governance. Digital agriculture research shows that technologies such as decision-support tools, sensors, robotics, and farm-management platforms reshape relationships among farmers, advisors, researchers, technology providers, and public or private institutions. Responsible agricultural AI therefore requires more than technical performance assessment:

it also requires lifecycle governance, context-sensitive institutional capacity, and explicit responsibilities for the actors who develop, provide, configure, interpret, and use AI-enabled systems [1-3]. When these interconnected elements influence agronomic decisions or physical farm operations, accountability cannot be located solely in the algorithm. It must also consider the conditions under which data were produced, the assumptions embedded in models, the design and monitoring of platforms, the interpretation of recommendations, the integration of machinery, and the ability of human actors to intervene.

The social and ethical literature on agricultural AI identifies recurring concerns involving privacy, bias, transparency, explainability, autonomy, changing labour relations, concentrated technological power, and uncertainty over who should answer for harmful or inappropriate outcomes [4]. These concerns do not mean that every agricultural AI failure produces legal liability, nor do they establish which party would be legally responsible in a particular jurisdiction. Liability is a legal determination that may depend on applicable law, contractual relationships, evidence, causation, standards of conduct, and the facts of a specific event. Accountability is broader. It concerns whether actors can explain decisions, document their contribution, justify system design and use, respond to identified failures, and participate in correction or remediation. Ethical responsibility concerns duties that may exist even where formal legal liability is uncertain, while operational accountability concerns the allocation of monitoring, intervention, maintenance, and incident-response functions within a working agricultural system.

A layered approach is needed because agricultural AI outputs frequently pass through several transformations before they influence a farm decision or physical action. Sensor readings may be collected by one provider, stored by another, transformed by a platform, analysed by a model developed elsewhere, displayed through an interface, interpreted by an advisor, and acted upon by a farmer or automated machine. At each transition, information may be lost, assumptions may become invisible, uncertainty may be compressed, and responsibility may become ambiguous. A prediction is not identical to an advisory recommendation, and an advisory recommendation is not identical to machinery execution. Similarly, the presence of a human reviewer does not automatically make oversight meaningful. Effective human control depends on whether the reviewer has sufficient information, competence, time, authority, interface support, and a realistic opportunity to reject, modify, escalate, or stop the system's output.

The objective of this article is to propose an original conceptual accountability framework for AI liability issues in precision agriculture across data, model, platform, advisory, machinery, and operational layers. The framework is designed to clarify actor roles, validation responsibilities, evidence trails, decision boundaries, monitoring duties, escalation pathways, and accountability gaps. It distinguishes accountability mapping from legal-liability determination and treats documentation, traceability, auditability, explainability, and human oversight as necessary but individually insufficient accountability mechanisms. The framework also introduces explicit boundaries against interpreting completion of an accountability exercise as proof of legal compliance, operational safety, certification, regulatory approval, or deployment readiness. Its intended contribution is therefore analytical and governance-oriented: it offers a structured way to ask who had control, knowledge, duties, evidence, and intervention capacity at each stage of an agricultural AI system.

AI Liability in Precision Agriculture

AI liability in precision agriculture is best approached initially as a problem of distributed accountability rather than as a predetermined legal conclusion. Empirical work on responsible AI in agriculture indicates that responsibility is negotiated through relationships among researchers, technology developers, institutions, collaborators, users, and affected communities, rather than being held by one clearly isolated actor [5]. This distributed pattern is especially relevant when an agricultural AI service combines third-party datasets, proprietary models, platform interfaces, professional advice, and machinery supplied by different organizations. A developer may control model architecture but lack authority over local deployment. A platform provider may determine interface defaults and update practices but not the final farm decision. An advisor may interpret an output without being able to inspect the model. A farmer may act on advice while lacking access to the data transformations or validation evidence behind it. The framework must therefore distinguish contribution,

control, knowledge, capacity, and decision authority instead of assuming that proximity to the final action is equivalent to complete responsibility.

Responsible and trustworthy AI provide useful governance concepts, but they should not be presented as labels that automatically resolve accountability. A multi-criteria farming framework demonstrates that responsible AI design may involve transparency, privacy, fairness, robustness, sustainability, stakeholder well-being, and farmer autonomy, with potential trade-offs among these objectives [6]. In accountability terms, this means that a system should not be assessed only through aggregate accuracy or efficiency. A technically accurate model may still lack documented provenance, communicate uncertainty poorly, create dependence on a platform, disadvantage underrepresented farm contexts, or encourage actions outside its validated use. Conversely, a transparent model may still be unreliable, insecure, or operationally inappropriate. Trustworthy AI should therefore be interpreted as an aspiration requiring evidence across technical, organizational, social, and operational dimensions rather than as a certification status or a guarantee that responsibility has been adequately allocated.

Precision-agriculture technologies may also redistribute expertise, benefits, burdens, and decision authority. Research on responsible innovation in precision agriculture shows that decision-support systems are shaped by design assumptions, institutional relationships, and unequal access to technical or agronomic knowledge [7]. These systems may influence whose expertise is treated as authoritative, which farming objectives are optimized, how uncertainty is communicated, and whether farmers can meaningfully challenge recommendations. Shared responsibility can be constructive when complementary duties are explicit—for example, when developers document model limitations, advisors evaluate local relevance, and farm operators retain clear decision authority. However, shared responsibility becomes an accountability problem when each actor assumes that another party completed the necessary validation, monitoring, explanation, or risk assessment. The concept should not become a mechanism for dispersing responsibility until no actor remains answerable for a material decision.

Accountability must also begin before model development or farm-level use. Responsible-innovation analysis of digital farming demonstrates that upstream choices about data selection, infrastructure, commercial priorities, and stakeholder inclusion can create uneven participation and unequal technological effects [8]. A system may exclude certain production settings because relevant data were unavailable, prioritize variables aligned with provider interests, or create dependencies through proprietary infrastructure. These choices can later appear as neutral technical conditions even though they reflect organizational decisions. The accountability framework therefore treats data architecture, technology procurement, system integration, and use-case definition as responsibility-bearing stages. At the same time, it establishes four boundaries: accountability mapping does not determine legal liability; documentation does not establish compliance; responsible-AI principles do not guarantee operational safety; and a completed conceptual framework does not demonstrate deployment readiness. These boundaries are necessary because accountability analysis may reveal responsibility pathways and evidence gaps, but legal, technical, and institutional conclusions require separate assessment.

Data-Level and Model-Level Accountability

Data-level accountability begins with identifying who collected, supplied, maintained, transformed, accessed, or transferred agricultural data and under what conditions. Farmers' reluctance to participate in smart-farming data arrangements has been linked to uncertainty about data access, control, subsequent use, and the legal or organizational rules governing sharing [9]. A data provider may generate raw information, but a data steward may determine retention, correction, access, or deletion, while an intermediary may aggregate or transform the data before model development. These roles should not be collapsed into a generic category of "data owner." Accountability requires records of collection purpose, source identity, measurement conditions, timestamps, units, permissions where applicable, and known limitations. Data quality responsibilities should address completeness, accuracy, timeliness, representativeness,

calibration, and missingness. Provenance should connect raw observations to transformations and derived datasets so that reviewers can reconstruct how material model inputs were produced.

Transparency about agricultural data use is also essential because accountability depends on whether affected actors can understand what is being collected, why it is needed, who receives it, and who may benefit from its use. Smart-farming research has shown that trust is weakened when farmers are not told how their data are used or how benefits are distributed among participating actors [10]. Data documentation should therefore record variables, sampling conditions, transformations, exclusions, sharing arrangements, and material limitations. Access controls should specify which actors can retrieve or modify data, while control records should identify who may combine, commercialize, transfer, correct, or delete them. Privacy review should extend across collection, transmission, storage, processing, and sharing rather than being treated as a one-time consent exercise. Cybersecurity responsibilities should likewise be allocated across devices, networks, platforms, credentials, storage services, and connected operational systems because a security failure may affect both information governance and physical farm operations.

Agricultural data accountability cannot be resolved through ownership language alone. Analysis of agricultural data governance shows that a narrow ownership debate may obscure the more practical questions of access, control, portability, reuse, stewardship, and the duties of actors holding or processing farm data [11]. The proposed framework therefore treats ownership as a concern to be documented, not as a sufficient allocation mechanism. A party may claim ownership while another party exercises practical control over storage, transfer, modification, or commercial use. Similarly, farmer consent or contractual acceptance does not necessarily establish that data practices are understandable, proportionate, secure, or accountable. A data-governance arrangement should identify decision rights, oversight functions, review procedures, retention expectations, complaint pathways, and mechanisms for correcting inaccurate records. It should also document the boundaries between farmer authority, platform control, intermediary functions, and institutional requirements without claiming that the framework itself establishes legal rights or compliance.

Model-level accountability concerns who developed, selected, adapted, validated, deployed, monitored, and communicated the AI model. Explainable-AI scholarship in agricultural analysis demonstrates that black-box predictions can limit scrutiny of how outputs were produced and why particular variables influenced a result [12]. Model developers should document objectives, features, training assumptions, evaluation methods, known limitations, prohibited uses, and dependencies. Model deployers should separately justify why a model is suitable for the intended agricultural context and configuration. Validation should distinguish internal testing from external validation, local validation, and staged field-validation planning. It should address error patterns, robustness, calibration, uncertainty, bias, fairness, and performance across relevant farm types, crops, locations, seasons, or production practices. Post-deployment responsibility should include data-drift and model-drift monitoring, version control, revalidation triggers, rollback procedures, and communication of changed limitations. Explainability and transparency can support review, but neither proves correctness. The framework therefore includes a no-model-responsibility-sufficiency boundary: model documentation, explanation, or validation alone cannot determine responsibility for the complete agricultural AI system. Table 1 summarises data-level and model-level accountability requirements for AI systems in precision agriculture.

Table 1. Data-Level and Model-Level Accountability Requirements in Precision Agriculture AI Systems: Data Providers, Data Stewards, Data Quality, Provenance, Ownership Concerns, Access, Control, Documentation, Governance, Privacy, Cybersecurity, Model Developers, Validation, Drift Monitoring, Bias, Fairness, and Responsibility Boundaries

Accountability component	Core responsibility question	Responsible actor or role	Required evidence or practice	Accountability function	Potential output	Accountability gap
Data provider	Who generated or supplied the data,	Farmer, farm operator, sensor	Source identity, collection context,	Establish data origin and answerability	Data-source record	Unverified or anonymous source

	and under what conditions?	provider, cooperative, public-data provider	timestamps, permissions, known limitations			
Data steward	Who maintains quality, access, correction, retention, and authorized use?	Farm organization, cooperative, research institution, platform operator	Stewardship policy, access register, correction process, retention schedule	Maintain controlled data management	Stewardship log	Stewardship duties are assumed but not allocated
Data intermediary	Who transfers, aggregates, brokers, or transforms data between actors?	Platform provider, cooperative, service provider, processor	Transfer records, transformation history, recipient list, role description	Preserve accountability across data movement	Data-flow record	Responsibility disappears during aggregation
Data collection	Was data collection tied to a defined and proportionate use?	Data provider, technology provider, farm operator	Collection protocol, purpose statement, sensor configuration	Connect collection to system purpose	Collection specification	Data collected without a defined purpose
Data quality	Who evaluates completeness, accuracy, timeliness, and representativeness?	Data steward, developer, domain specialist	Quality thresholds, calibration records, missing-data analysis, anomaly review	Prevent unreliable inputs from entering models	Data-quality report	No actor accepts responsibility for defects
Data provenance	Can the source and transformation history of each material dataset be reconstructed?	Data steward, intermediary, developer	Provenance chain, version identifiers, transformation logs	Support traceability and causal investigation	Provenance record	Broken chain between raw and model-ready data
Data documentation	Are variables, units, sampling methods, exclusions, and limitations described?	Data steward, developer	Data dictionary, metadata, change log, limitation statement	Make data interpretable and reviewable	Dataset documentation	Data exist without contextual meaning
Data access	Who may access particular data and for which purpose?	Data steward, platform provider,	Role-based permissions, access logs,	Restrict and retrospectively examine access	Access-control matrix	Excessive or undocumented permissions

Model deployer	Who selected and configured the model for the agricultural use case?	Platform provider, technology provider, system integrator, farm organization	Deployment rationale, configuration record, intended-use statement	Connect a general model to a specific use	Deployment record	Developer and deployer duties are conflated
Model documentation	Are intended uses, prohibited uses, inputs, outputs, limitations, and dependencies recorded?	Developer and deployer	Model record, version history, limitation statement, dependency list	Support scrutiny and appropriate use	Model documentation	Records are incomplete, outdated, or inaccessible
Model validation	Who evaluates error, calibration, robustness, uncertainty, and failure patterns?	Developer, independent evaluator where feasible, domain specialist	Prespecified metrics, test sets, error analysis, robustness assessment	Determine whether evidence supports intended use	Validation report	Performance claims lack contextual analysis
External validation	Was performance assessed outside the development-controlled data environment?	Independent evaluator, research partner, deployer	External dataset, evaluation protocol, context comparison	Test transportability beyond development conditions	External-validation record	Internal performance is treated as universal
Local validation	Does the model perform appropriately in the relevant farm, crop, soil, climate, and management context?	Deployer, agronomist, farm operator, local evaluator	Local data, contextual review, uncertainty assessment	Evaluate local suitability	Local-validation statement	Generic model used without local evidence
Field-validation planning	What staged evidence and oversight are required before outputs influence operations?	Deployer, farm organization, system integrator, domain specialist	Pilot protocol, stop criteria, oversight plan, harm-monitoring process	Structure cautious progression toward operational use	Field-validation plan	Retrospective evidence is treated as field proof
Model-drift monitoring	Who identifies deterioration or changed model behaviour over time?	Model deployer, platform provider	Performance dashboard, thresholds, review schedule,	Detect post-deployment degradation	Drift alert and review record	No actor owns continuing performance

			rollback process			
Data-drift monitoring	Who monitors changes in sensors, environments, practices, seasons, or input distributions?	Data steward, deployer, system integrator	Distribution checks, sensor-change logs, context indicators	Detect invalidated assumptions	Data-drift alert	Changed conditions remain invisible
Bias and fairness assessment	Which groups, farm types, crops, or regions may receive systematically poorer performance?	Developer, deployer, domain and social reviewers	Subgroup analysis, representation review, impact assessment	Identify unequal errors and burdens	Bias and fairness report	Aggregate metrics conceal uneven impacts
Robustness	How does the model behave under noise, missing data, unusual conditions, or component variation?	Developer, deployer, evaluator	Stress tests, sensitivity analysis, failure thresholds	Assess stability beyond average conditions	Robustness record	Normal-condition testing is treated as sufficient
Explainability and transparency	Can relevant users understand the basis, limits, and status of an output?	Developer, deployer, platform provider	Audience-specific explanation, fidelity review, uncertainty statement	Support challenge and interpretation	Explanation record	Explanation is persuasive but unfaithful
Uncertainty communication	Are confidence, limitations, and out-of-distribution conditions conveyed clearly?	Developer, platform provider, advisor	Calibrated uncertainty, plain-language notice, escalation threshold	Prevent false certainty	Uncertainty statement	Precise presentation conceals weak evidence
No model-responsibility sufficiency boundary	Can model evidence alone determine responsibility or legal liability?	All framework users	Explicit limitation and cross-layer review	Prevent model-centric responsibility claims	Boundary statement	Model quality is treated as complete accountability

Platform and Advisory System Responsibility

Platform responsibility concerns the organizations that host, configure, update, monitor, and mediate access to agricultural AI services. Research on cloud-based farm advisory services shows that digital systems reshape how farmers and advisors obtain information, interpret evidence, and coordinate decisions [13]. A platform may combine data ingestion, model execution, interface design, alerting, storage, and communication functions even when separate providers supply individual components. Accountability therefore requires distinguishing the platform provider from the

technology provider, system integrator, and service provider. The platform provider may control governance rules and updates; the technology provider may supply a model or sensor; the integrator may connect otherwise separate components; and the service provider may maintain or configure the system. Each role should have documented responsibilities, limitations, monitoring duties, escalation contacts, and evidence-retention practices. The existence of contracts or service terms does not by itself demonstrate that these responsibilities are understandable, technically adequate, or responsibly implemented.

Agricultural advisory responsibility should be mapped through the wider knowledge and advice network rather than assigned only to the individual who communicates a recommendation. Digitalization increasingly connects farmers, advisors, agronomists, agribusinesses, platform providers, researchers, consumers, and governance institutions through shared information infrastructures [14]. Within this network, the manuscript distinguishes model output from advisory output. A model output may be a probability, classification, estimate, or detected pattern. An advisory output is an interpreted recommendation communicated for consideration in a farm context. Agricultural advisors and agronomists may add domain knowledge, compare the output with local observations, identify implausible assumptions, and communicate limitations. However, advisor review should be required according to the consequence and uncertainty of the decision rather than treated as a universal liability-transfer mechanism. A professional review does not automatically make an unvalidated model appropriate, and the absence of specialist review does not mean that upstream developers or platform providers have no continuing responsibilities.

Interface design, platform monitoring, alerting, and escalation are accountability-bearing functions because platforms shape how users perceive and act upon AI outputs. Digital farming platforms may create path dependence or constrain available choices through defaults, categories, recommended workflows, and infrastructural lock-in [15]. An accountable interface should distinguish observations, predictions, recommendations, warnings, and machine commands. It should communicate uncertainty and limitations without presenting probabilistic outputs as certain instructions. Alert systems should use understandable severity levels and identify the action expected from the recipient. Monitoring should address reliability, abnormal outputs, complaints, security events, repeated overrides, and signs of model or data drift. Escalation pathways should identify who must be contacted when an output exceeds a confidence threshold, conflicts with field observations, raises safety concerns, or cannot be interpreted responsibly. These mechanisms support accountability only when actors have authority and resources to respond; passive logging without assigned response duties is insufficient.

Platform governance must also examine data policies, surveillance capacity, dependencies, and the practical distribution of control. Critical analysis of agricultural platforms shows that contractual terms and data policies can support extensive monitoring and extraction while farmers retain limited visibility into downstream data uses or platform practices [16]. Accountability therefore requires review of update authority, data flows, access rules, monitoring practices, interface defaults, commercial dependencies, and exit or portability conditions. Human-in-the-loop review must be meaningful: advisors or farm operators need adequate information, competence, time, and authority to question, modify, reject, or escalate an output. Farmer autonomy likewise requires more than formal consent; it includes the practical ability to understand recommendations, contest assumptions, seek alternative advice, override defaults, and avoid unreasonable dependence. The framework retains two explicit boundaries. First, farmer acceptance, advisor review, or operator action does not independently determine advisory liability. Second, platform terms, disclaimers, documentation, and audit logs do not by themselves establish that platform responsibility has been adequately fulfilled.

Machinery, Automation, and Operational Risk

Agricultural robotics and automated machinery extend AI accountability from informational outputs into physical execution. Agricultural robots may redistribute control and responsibility among designers, model developers, robotics providers, machinery manufacturers, system integrators, farm operators, supervisors, and institutions, while systems-oriented design research shows that responsible operation depends on interactions across human, cyber, and physical

components. Autonomous agri-food technologies also create unresolved questions concerning supervision, intervention, and responsibility when machines perform tasks with limited direct control [17-19]. Accountability analysis should therefore distinguish the manufacturer responsible for mechanical and control-system characteristics, the robotics provider supplying perception or planning functions, the integrator connecting software and machinery, and the farm operator responsible for defined inspections or supervisory actions. These responsibilities may overlap, but they should not remain implicit. The designation of a machine as autonomous does not identify which actor is legally liable for a harmful outcome, nor does it establish that the operating conditions, oversight arrangements, or safeguards were adequate.

Machinery-layer responsibility must be interpreted in relation to the particular use case and the relationships among actors, technologies, environments, and affected parties. Case-based analysis of agri-food robots indicates that ethical and responsibility questions differ across applications because systems involve distinct tasks, users, physical environments, levels of autonomy, and opportunities for human control [20]. A robotic weeding function, harvesting system, livestock-management device, or processing robot may rely on different sensing, decision, and actuation pathways. The accountability framework therefore requires a documented sensor-to-actuator chain showing how observations are collected, processed, converted into model outputs, translated into control commands, and executed by machinery. Material system states, software versions, configuration changes, intervention events, and actuator responses should be traceable. This evidence can support investigation and organizational learning, but it cannot independently establish legal causation or responsibility.

Operational accountability also requires safeguards that address more than predictive model accuracy. Safety research on automated agricultural machinery emphasizes perception, risk assessment, risk mitigation, human factors, and ergonomics as interdependent dimensions [21]. A model may classify an object correctly while a communication delay, integration fault, control-system error, or actuator defect produces unsafe behavior. Conversely, an operator may receive an alert but lack sufficient time, visibility, competence, or authority to intervene. Fail-safe design should specify how the system responds to sensor failure, uncertain inference, communication loss, power interruption, software malfunction, or conflicting commands. Where appropriate to the system, emergency stopping, safe-state transitions, bounded actuation, geofencing, fault diagnostics, and controlled restart procedures should be defined and assessed. Human supervisory control should be meaningful rather than symbolic, with realistic intervention assumptions and clear mode indications.

Maintenance, cybersecurity, operational monitoring, and incident reporting complete the machinery accountability pathway. Manufacturers, providers, service organizations, and farm operators may hold different duties for calibration, inspection, software updates, component replacement, credential protection, network security, and record preservation. Monitoring should identify abnormal behavior, repeated overrides, sensor degradation, unexpected path planning, control instability, or operation outside defined conditions. Incident and near-miss procedures should preserve relevant data, system states, versions, maintenance records, and human actions so that failures can be examined across the complete system. Nevertheless, logging does not allocate blame, and incident reporting does not constitute legal adjudication. The proposed framework therefore includes a no-operational-safety-guarantee boundary and a no-autonomous-action-responsibility-resolution boundary: accountability mapping may clarify who controlled or documented particular functions, but it does not certify machinery safety or independently determine responsibility for autonomous action.

Liability Gaps Across Agricultural AI Systems

Liability and accountability gaps emerge when responsibility is lost at the boundaries connecting data, models, platforms, advisory processes, machinery, and farm operations. Smart-farming ethics research identifies unresolved questions concerning privacy, data control, transparency, autonomy, power, and the distribution of responsibility among technology providers and agricultural users [22]. A data provenance gap may prevent reviewers from identifying whether an error originated in collection or transformation. A validation responsibility gap may arise when developers assume that deployers will conduct local assessment while deployers rely on general development results. A platform responsibility

gap may occur when interface design, updates, or monitoring practices materially influence use but are treated as neutral service functions. Advisory interpretation and machinery execution create further transitions at which outputs may change status from prediction to recommendation and from recommendation to physical action. **Figure 1** illustrates how liability and accountability gaps can emerge across data, model, platform, advisory, machinery, and operational layers in precision agriculture AI systems.

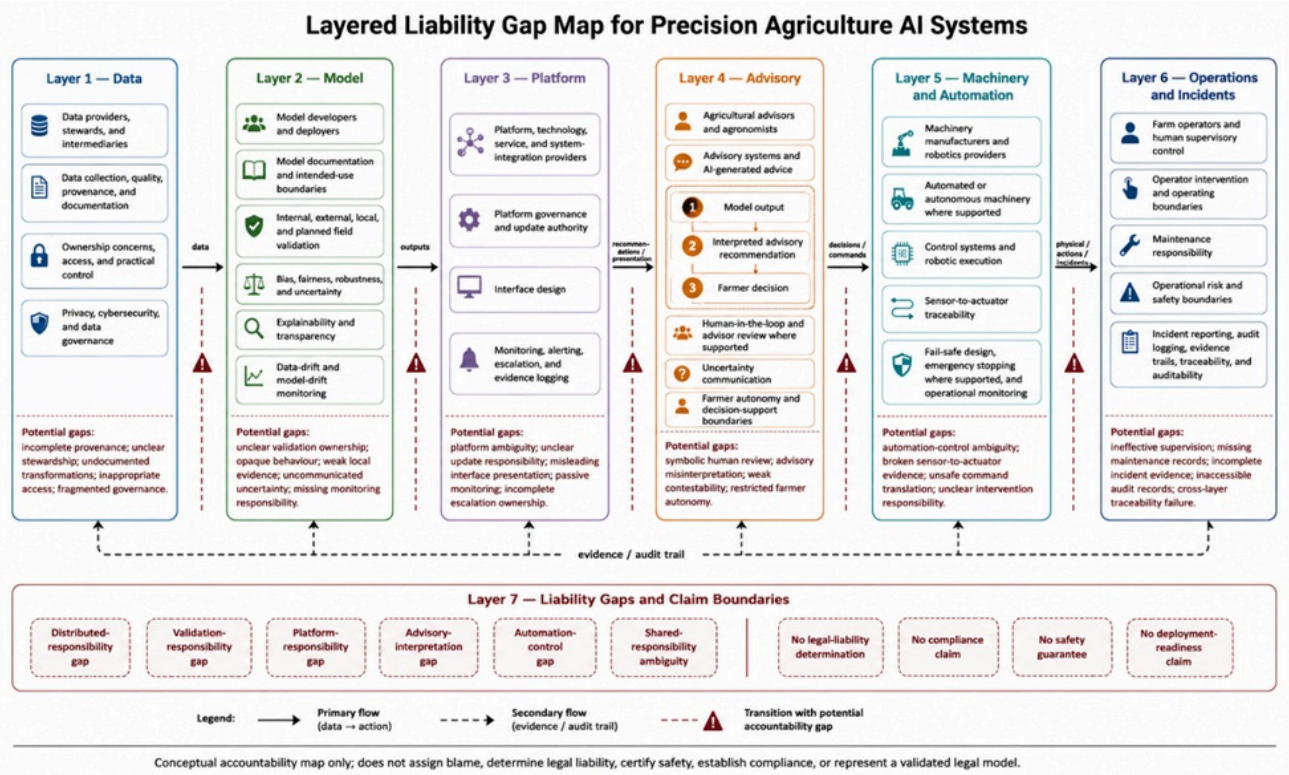


Figure 1. Layered Liability Gap Map for Precision Agriculture AI Systems

Alt-text description:

A conceptual layered map showing agricultural AI accountability gaps across data providers, model developers, platform providers, advisory actors, machinery systems, farm operators, incident reporting, traceability, and auditability.

Distributed responsibility gaps are intensified by unequal control over data, infrastructure, technical expertise, and market access. Critical research on digital agricultural technologies shows that concentrated technological and informational power can shape who defines system objectives, controls data flows, benefits from automation, and bears the burdens of failure or dependency [23]. Actors with the greatest formal or practical control may be distant from farm-level outcomes, while farmers and operators may be highly exposed to consequences without having access to model logic, platform governance records, or system-level evidence. Shared responsibility is therefore not necessarily balanced responsibility. The framework asks which actor possessed relevant knowledge, who could change a design or operating condition, who had authority to interrupt use, who was expected to monitor performance, and who retained evidence after an incident. These questions support accountability analysis without presuming that organizational influence is equivalent to legal fault.

Additional gaps arise when human oversight, interface design, and farmer autonomy are treated as secondary concerns. Responsible-innovation scholarship emphasizes anticipation, inclusion, reflexivity, and responsiveness as means of identifying affected interests and revising technology arrangements before harms become entrenched [24]. A human

oversight gap exists where a named reviewer lacks the competence, time, information, or authority required to challenge an output. An interface ambiguity gap occurs when users cannot tell whether a displayed result is an observation, probability, advisory recommendation, warning, or control command. Farmer-autonomy gaps may arise through platform lock-in, restrictive defaults, inaccessible explanations, weak contestability, or dependence on a provider for data portability and service continuity. These are accountability problems because they affect practical control and the distribution of decision authority, even where a farmer has formally accepted the service.

Privacy, cybersecurity, drift, incident evidence, traceability, and auditability create lifecycle accountability gaps that may remain hidden until a system fails. Privacy review of smart farming shows that risks can arise during collection, communication, storage, processing, and sharing, requiring responsibility across the complete data lifecycle [25]. Data drift may result from changes in climate, sensors, practices, crop conditions, or farm management, while model drift may follow updating, feedback effects, or changing relationships between inputs and outcomes. An incident evidence gap arises when versions, logs, human decisions, and machinery states are not preserved. An auditability gap arises when records exist but authorized reviewers cannot meaningfully access or interpret them. A traceability gap exists when evidence cannot be linked across layers. **Table 2** maps platform, advisory, machinery, automation, operational-risk, and liability-gap concerns across agricultural AI systems.

Table 2. Platform, Advisory, Machinery, Automation, Operational-Risk, and Liability-Gap Concerns Across Agricultural AI Systems: Platform Governance, Advisory Responsibility, Human Oversight, Machinery Automation, Robotic Execution, Operational Monitoring, Incident Evidence, Traceability, Auditability, Shared Responsibility, and Legal-Claim Boundaries

Layer, component, or gap	Core accountability question	Responsible actor or role	Required evidence or condition	Potential output or consequence	Failure or responsibility gap	Safeguard or monitoring need	
Platform provider	Who controls platform rules, updates, access, and data flows?	Platform provider	Governance record, update history, data-flow map, service limitations	Platform responsibility profile	Platform treated as neutral infrastructure	Governance and change monitoring	also c le
Technology provider	Who supplies the model, sensor, interface, or connectivity component?	Technology provider	Component documentation, intended use, known limitations	Provider-role record	Component duties are unclear after integration	Configuration and dependency review	do is c
System integrator	Who connects data, models, platforms, interfaces, and machinery?	System integrator	Architecture record, integration tests, dependency map	Integration assurance record	Failures fall between component providers	End-to-end testing and change control	I ev nc sa
Service provider	Who configures, hosts, maintains, or supports the service?	Service provider	Service scope, maintenance log, support and escalation contacts	Service-responsibility statement	Responsibility ends ambiguously after installation	Service monitoring and escalation	Se ac

Platform governance	Who approves consequential changes and access rules?	Platform provider and governance body	Decision-rights charter, approval record, review process	Governance decision log	No accountable authority for changes	Periodic governance review	G
Platform monitoring	Who detects abnormal outputs, misuse, complaints, or reliability problems?	Platform operator, deployer, service provider	Monitoring indicators, thresholds, complaint log, response procedure	Monitoring report	Monitoring exists without response ownership	Assigned escalation and correction duties	I
Interface design	Does the interface distinguish prediction, advice, warning, and command?	Platform provider, interface team, integrator	Interface specification, terminology controls, usability assessment	Interface-assurance record	Users misinterpret output status	User-centered testing and clear mode labels	cla
Advisory system	Is the system descriptive, predictive, prescriptive, or controlling?	Platform provider, deployer, advisory organization	Function classification, intended-use statement	Advisory classification	Advisory tools function as implicit control systems	Decision-role review	C
AI-generated advice	Are assumptions, uncertainty, and limitations communicated?	Model deployer, platform provider, advisor	Explanation, uncertainty statement, source and version records	Advice evidence package	Advice appears certain or context-free	Risk-tiered review and escalation	A
Agricultural advisor or agronomist	Who evaluates contextual and agronomic plausibility?	Advisor or agronomist	Review notes, contextual assumptions, conflict checks	Reviewed recommendation	Professional review becomes symbolic	Competency and review-quality monitoring	R
Human oversight	Does the human have information, time, competence, and authority to intervene?	Advisor, operator, supervisor	Training, workload assessment, override authority, interface support	Human-review record	Human presence without meaningful control	Review of overrides and intervention capacity	alc
Farmer autonomy	Can the farmer understand, reject, contest, or exit the arrangement?	Platform provider, advisor, farm organization	Choice architecture, portability, override and review options	Autonomy assessment	Defaults or dependency restrict practical choice	Contestability and dependency review	a
Machinery manufacturer	Which physical, control, and	Machinery manufacturer	Design limits, hazard	Machinery responsibility	Mechanical and software	Safety design and	Do

	safety functions remain under manufacturer responsibility?		analysis, maintenance requirements	record	duties are blurred	maintenance monitoring	
Robotics provider	Who supplies perception, planning, navigation, or autonomous-task functions?	Robotics provider	Algorithm, sensor, operating-domain, and test records	Robotics responsibility record	Autonomous functions are insufficiently bounded	Performance monitoring and safe-state behavior	
Control system	Who verifies state transitions, limits, and command logic?	Control developer, manufacturer, integrator	Control architecture and verification evidence	Control assurance record	Correct predictions produce unsafe commands	Diagnostics and bounded control	acc co
Sensor-to-actuator chain	Can sensing, inference, command, and execution be reconstructed?	Sensor provider, developer, integrator, manufacturer	Time-synchronized logs and version records	End-to-end evidence trail	Causal pathway is broken	Traceability and latency monitoring	T es
Human supervisory control	Can the operator understand system state and intervene effectively?	Farm operator or supervisor	Situation-awareness support, communication reliability, override capacity	Supervision record	Intervention is delayed or impossible	Clear modes, alerts, and tested override	su i
Fail-safe design	What happens when sensing, communications, software, power, or control fails?	Manufacturer, robotics provider, integrator	Failure-mode analysis, safe-state definition, fault testing	Fail-safe specification	System continues unsafe action	Redundancy, safe stop, bounded degradation	cla
Emergency stop where supported	Can hazardous movement be stopped promptly and predictably?	Manufacturer, integrator, operator	Accessible stop mechanism, testing, controlled reset	Stop-test record	Failure to stop or unsafe restart	Routine inspection and testing	E sto r f
Maintenance responsibility	Who calibrates, patches, repairs, and records changes?	Manufacturer, service provider, farm operator	Maintenance schedule, calibration log, change-control record	Maintenance status record	Degradation or updates remain undocumented	Preventive maintenance and post-change testing	M d ov
Operational monitoring	Who monitors abnormal or	Operator, provider,	Health indicators, thresholds,	Operational monitoring report	Abnormal behavior is	Assigned intervention	f i

	degraded behavior?	platform operator	response duties		detected but not acted upon	and escalation	
Cybersecurity	Could unauthorized access alter data, commands, or machine state?	Provider, integrator, platform operator, farm operator	Threat model, authentication, patching, recovery plan	Cybersecurity responsibility map	Security duties are fragmented	Intrusion detection and recovery testing	Cy re ne c
Incident evidence gap	Are versions, states, decisions, and actions preserved after an incident?	Operator, provider, manufacturer	Incident protocol and evidence-preservation procedure	Investigable incident record	Evidence is missing or overwritten	Protected reporting and retention	p all
Auditability gap	Can an authorized reviewer assess relevant records and controls?	Provider, deployer, governance body	Audit access, structured logs, review procedures	Audit record	Proprietary or unusable evidence blocks scrutiny	Proportionate audit-access design	A c
Traceability gap	Can outputs and actions be linked to actors, versions, and decisions?	All responsible organizations	Shared identifiers and linked records	Traceability chain	Records cannot be joined across layers	Periodic traceability tests	T s e re
Data or model drift gap	Who detects changing inputs or deteriorating behavior?	Data steward, model deployer, platform provider	Baselines, drift indicators, thresholds, revalidation rules	Drift alert	Silent performance deterioration	Monitoring, rollback, and reassessment	de do
Shared responsibility ambiguity	Are duties complementary, overlapping, conflicting, or absent?	All involved organizations	Responsibility-allocation and conflict map	Shared-responsibility profile	Actors defer action to one another	Joint governance and escalation rules	re re e
No legal-liability determination boundary	Is accountability mapping being treated as legal adjudication?	All framework users	Explicit limitation statement	Non-determination notice	Unsupported legal conclusions	Separate legal interpretation where applicable	Th e le
No compliance claim boundary	Is documentation being	All framework users	Explicit compliance limitation	Compliance-boundary notice	False assurance	Independent institutional and legal assessment	F c

represented as
compliance?

Proposed Accountability Framework

The proposed framework conceptualizes accountability as a relational and institutional process requiring answerability, evidence, assessment, correction, and the capacity to respond to identified problems. General AI accountability scholarship emphasizes that algorithms cannot be meaningfully held to account in isolation from the organizations and actors that develop, deploy, oversee, and use them, while operational ethics research shows that principles require concrete lifecycle practices and assigned procedures [26-28]. Adapted to precision agriculture, this means that accountability should be mapped across the full system rather than concentrated on model output or the final farm decision. The framework is not presented as an empirical finding or legal instrument. It is a proposed analytical structure for identifying who had relevant control, knowledge, authority, documentation duties, validation obligations, monitoring capacity, and opportunities to intervene.

The first stage defines the agricultural AI use case, intended decision, affected environment, consequence level, and prohibited uses. Stakeholder and role mapping then identifies farmers, farm operators, data providers, data stewards, intermediaries, model developers, model deployers, platform providers, technology providers, system integrators, advisors, agronomists, machinery manufacturers, robotics providers, service providers, cooperatives where supported, and relevant governance, insurance, or supply-chain actors where the evidence and context justify their inclusion. These stages should reflect the responsible-AI principles of beneficence, non-maleficence, autonomy, justice, and explicability while recognizing that such principles require contextual interpretation [29]. Role mapping should document formal duties and practical control because contractual labels may not correspond to who can access data, alter a model, change a platform default, stop machinery, preserve evidence, or respond to an incident.

The second stage maps accountability across data and model layers. Data mapping assigns responsibility for collection purpose, quality, provenance, documentation, access, control, privacy, cybersecurity, transfer, and retention. Model mapping assigns responsibility for development choices, model documentation, internal testing, external validation, local validation, field-validation planning, bias and fairness assessment, robustness, explainability, uncertainty communication, deployment configuration, and drift monitoring. Algorithm-accountability research indicates that evaluation should include the values, assumptions, organizational choices, and consequences embedded in system design and use rather than treating the algorithm as an independent moral or organizational actor [30]. The framework consequently asks not only whether a model performed well, but who selected its objective, whose data were represented, which errors were prioritized, where limitations were communicated, and who had authority to suspend or revise deployment.

The third stage maps platform, advisory, machinery, and operational responsibilities. Platform mapping covers governance rules, access arrangements, updates, interface design, alerting, monitoring, logging, service dependencies, and escalation. Advisory mapping distinguishes analytical outputs from interpreted recommendations and identifies when advisor or agronomist review is supported by the consequence and context of the decision. Machinery mapping addresses perception, control, robotic execution, integration, maintenance, fail-safe behavior, emergency intervention where supported, and sensor-to-actuator traceability. Operational-risk mapping identifies abnormal states, operating-domain limits, supervisory duties, stop conditions, cybersecurity dependencies, and incident-response responsibilities. Human oversight is allocated according to actual information, competence, authority, workload, and intervention capacity rather than through a generic human-in-the-loop designation.

The final stage designs the evidence trail and governance feedback cycle. It specifies documentation, versioning, traceability, auditability, validation records, review records, escalation events, incident evidence, data- and model-drift alerts, corrective actions, and framework updates. Privacy and cybersecurity duties are reassessed as systems, providers, and data flows change. Farmer autonomy is reviewed through explanation, contestability, portability, override

capacity, and dependency. Remaining validation, responsibility, or evidence gaps are recorded for institutional, technical, or legal examination where applicable. **Table 3** presents the proposed accountability framework across data, model, platform, advisory, machinery, and operational layers in precision agriculture AI systems. **Figure 2** presents the proposed accountability framework for precision agriculture AI systems, integrating role mapping, evidence trails, validation responsibilities, oversight duties, incident response, traceability, auditability, and decision boundaries across data, model, platform, advisory, machinery, and operational layers.

Table 3. Proposed Accountability Framework for AI Liability in Precision Agriculture: Use-Case Definition, Stakeholder Role Mapping, Data-Layer Accountability, Model-Layer Accountability, Platform Responsibility, Advisory Responsibility, Machinery Responsibility, Operational Risk, Human Oversight, Validation Responsibility, Evidence Trails, Traceability, Auditability, Incident Response, Drift Monitoring, Farmer Autonomy, and Claim Boundaries

Framework stage	Core purpose	Required input	Accountability function	Potential output	Validation or assessment need	Failure risk	F m
Agricultural AI use-case definition	Define the problem, decision role, users, context, and consequence level	Use-case statement, intended outputs, operating environment	Prevent vague purposes and function creep	Approved use-case profile	Domain and stakeholder review	System used beyond its stated purpose	Pe rea
Stakeholder and role mapping	Identify actors with control, knowledge, duties, or exposure	Actor inventory and system architecture	Establish prospective answerability	Stakeholder–role map	Review with affected actors	Hidden intermediaries or missing actors	Up se
Data-layer accountability mapping	Allocate collection, quality, provenance, access, control, privacy, and security duties	Data-flow and source records	Establish data-level responsibility	Data accountability map	Data-governance assessment	Data defects remain ownerless	pr re
Model-layer accountability mapping	Allocate development, documentation, validation, explanation, and drift duties	Model architecture and lifecycle record	Establish model-level answerability	Model accountability map	Technical and domain assessment	Model evidence is mistaken for system evidence	Re ar
Platform-layer responsibility mapping	Clarify governance, updates, access, monitoring,	Platform architecture and governance records	Identify platform-provider responsibilities	Platform responsibility map	Organizational and technical review	Platform treated as neutral	C ch m f

	interface, and service duties						
Advisory-layer responsibility mapping	Distinguish model output, professional interpretation, and farm decision	Advisory workflow and output classification	Allocate interpretation and communication duties	Advisory responsibility map	Agronomic and usability review	Advice presented without context	Fa
Machinery-layer responsibility mapping	Allocate sensing, control, actuation, maintenance, and safety duties	Machinery and robotics architecture	Establish physical-execution accountability	Machinery responsibility map	Engineering and operational assessment	Harm attributed only to the final action	Ma
Operational-risk mapping	Identify hazards, dependencies, abnormal states, and response duties	Hazard scenarios and operating-domain description	Connect risks to responsible controls	Operational-risk register	Scenario and failure-mode review	Combined failures are overlooked	N
Human oversight allocation	Specify who reviews, supervises, overrides, escalates, and stops	Risk tiers, workflows, authority structure	Make human control meaningful	Oversight allocation record	Competency, workload, and control assessment	Symbolic human-in-the-loop arrangements	Over
Validation responsibility allocation	Assign internal, external, local, and field-validation duties	Intended-use and consequence profile	Prevent validation gaps	Validation responsibility plan	Independent review where appropriate	Each actor assumes another validated	Re
Documentation and evidence-trail design	Define material records, versions, decisions, and retention	System maps and responsibility allocations	Support reconstruction and answerability	Evidence-trail specification	Completeness and accessibility audit	Records are incomplete or unusable	A
Traceability design	Link data, model, platform, advice, control, and action	Identifier and logging schema	Reconstruct system pathways	Traceability architecture	End-to-end technical testing	Records cannot be connected across layers	tr
Auditability design	Enable authorized	Access rules, structured	Support independent or	Auditability plan	Governance and technical	Evidence exists but	Au

	scrutiny of records, controls, and decisions	records, review procedures	institutional review		assessment	cannot be meaningfully reviewed	c
Escalation and incident response design	Define detection, stopping, notification, investigation, and remediation	Risk thresholds, contact structure, evidence protocol	Coordinate response to uncertainty or failure	Escalation and incident plan	Simulation or tabletop assessment	Delayed response or evidence loss	C
Drift monitoring responsibility	Assign indicators, thresholds, review frequency, and responses	Baseline data and performance measures	Maintain post-deployment vigilance	Drift-monitoring plan	Statistical and domain review	Silent deterioration	rol re
Cybersecurity and privacy responsibility review	Allocate protection across data and connected operational systems	Data flows, networks, threat and privacy assessments	Protect information and operational integrity	Security and privacy responsibility map	Specialist review and periodic testing	Gaps between farm, device, and platform duties	Vu ar f
Farmer autonomy and decision-boundary review	Assess understanding, choice, override, contestability, and dependence	Interfaces, service arrangements, portability conditions	Preserve practical farmer agency	Autonomy and decision-boundary statement	Farmer-centered usability and governance review	Lock-in or nominal consent	C e
Liability-gap identification	Record unresolved, overlapping, or missing responsibility pathways	All layer maps and evidence records	Surface issues requiring further assessment	Liability-gap register	Multidisciplinary review	Framework creates false certainty	Ga rea
Governance review and framework updating	Revise roles, controls, evidence, and boundaries as systems change	Monitoring, incidents, complaints, validation, service changes	Maintain accountability relevance	Updated framework record	Periodic stakeholder and independent review	Outdated responsibilities persist	rev
No legal-liability determination boundary	Prevent conceptual mapping from	Explicit limitation statement	Preserve legal-adjacent caution	Non-determination notice	Separate legal interpretation where applicable	Unsupported blame allocation	F I

	becoming adjudication						
No compliance claim boundary	Prevent framework completion from being presented as compliance	Explicit limitation statement	Avoid unsupported compliance claims	Compliance-boundary notice	Separate institutional and jurisdictional assessment	Documentation is equated with compliance	Up rec
No safety-guarantee boundary	Prevent mapping from replacing engineering safety assessment	Explicit limitation and assessment requirement	Avoid unsupported safety assurance	Safety-boundary notice	Independent engineering assessment	Framework substitutes for testing	Ino as f
No deployment-readiness boundary	Prevent framework completion from being treated as operational readiness	Validation, monitoring, oversight, and institutional requirements	Maintain cautious interpretation	Deployment-readiness limitation	Separate empirical and institutional assessment	Premature use	as f

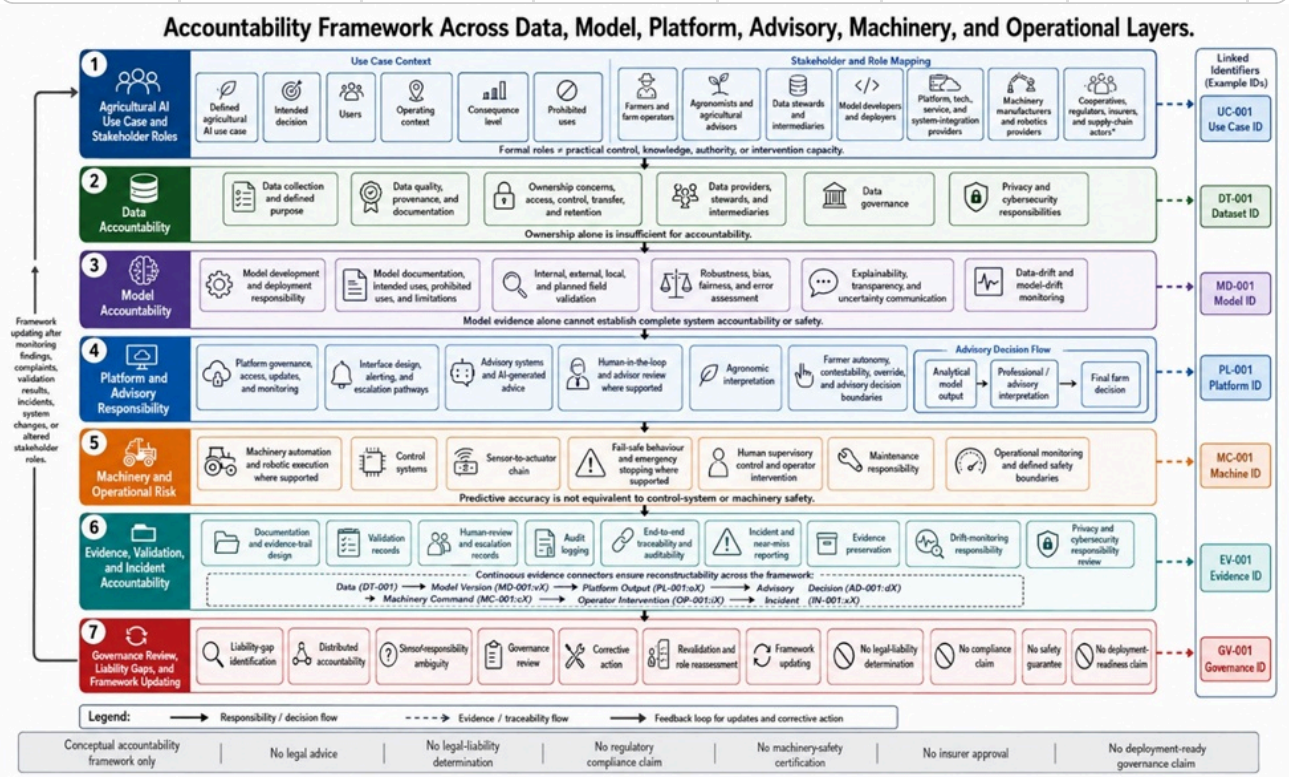


Figure 2. Accountability Framework Across Data, Model, Platform, Advisory, Machinery, and Operational Layers

Alt-text description:
A conceptual accountability framework showing precision agriculture AI use-case definition and stakeholder mapping

connected to data, model, platform, advisory, machinery, and operational accountability layers, with validation, oversight, evidence trails, traceability, auditability, incident response, and decision boundaries.

Policy and Managerial Implications

For policymakers and governance institutions, the framework suggests that agricultural AI discussions should address cross-layer responsibilities rather than focus exclusively on model transparency or the conduct of end users. Policy development may benefit from distinguishing duties associated with data stewardship, model validation, platform governance, advisory interpretation, machinery integration, and incident evidence. Responsible-innovation approaches support participation by affected stakeholders and continuing review as agricultural technologies and relationships change [24]. Conceptually, governance processes could encourage clear role descriptions, accessible evidence trails, proportionate auditability, complaint and escalation pathways, and preservation of farmer autonomy. These implications are not regulatory prescriptions and do not identify a universally appropriate legal allocation. Cooperatives, insurers where relevant, and supply-chain stakeholders may participate in documentation or risk discussions when supported by context, but their involvement should not be assumed to transfer responsibility or establish legal obligations.

For managers of farms, advisory organizations, technology providers, platforms, and service operations, the framework emphasizes role clarity before implementation and reassessment throughout system use. Data stewards should know who verifies quality, provenance, access, retention, privacy, and cybersecurity. Model developers and deployers should separately document development evidence, intended use, local suitability, monitoring, and revalidation responsibilities. Platform providers should assign governance, update, alerting, complaint, and incident-response functions rather than relying on general terms or disclaimers. Advisory organizations should define when domain review is expected and ensure that reviewers have adequate information and authority. Machinery manufacturers, robotics providers, integrators, and operators should clarify control modes, operating limits, maintenance, fail-safe functions, monitoring, and evidence preservation. Automated-machinery safety evidence supports attention to perception, risk mitigation, and human factors, but implementation decisions require system-specific engineering and institutional assessment [21].

For researchers, the framework identifies a research agenda concerning the empirical distribution of responsibility across agricultural AI ecosystems. Future studies could examine whether accountability records are understandable and usable, whether local validation responsibilities are fulfilled, how advisors interpret uncertainty, whether farmers can meaningfully challenge platform outputs, how drift is detected, and whether incident evidence can be reconstructed across organizational boundaries. Privacy and cybersecurity should be studied as linked lifecycle responsibilities rather than isolated technical controls [25]. Comparative work could also investigate how farm scale, infrastructure, crop or livestock context, service models, and institutional capacity affect meaningful oversight and farmer autonomy. These are proposed research and managerial implications, not legal, insurance, procurement, compliance, machinery-operation, platform-selection, agronomic, or deployment instructions.

Conclusion

This article proposes a conceptual accountability framework for examining AI liability issues across data, model, platform, advisory, machinery, and operational layers in precision agriculture. Its central contribution is to replace model-centered or single-actor explanations with a structured analysis of distributed accountability, role allocation, validation responsibility, documentation, evidence trails, traceability, auditability, human oversight, operational safeguards, incident response, and governance updating. The framework distinguishes data providers from stewards and intermediaries, developers from deployers, platforms from advisors, and advisory outputs from machinery execution. It also identifies accountability gaps caused by incomplete provenance, opacity, unclear validation ownership, platform ambiguity, weak human control, fragmented incident evidence, and untraceable physical action. These mappings may support governance planning and policy discussion, but they do not independently determine legal liability, assign blame, establish compliance, certify safety, or demonstrate deployment readiness. AI liability in precision agriculture should therefore be examined through the

complete chain of actors, technical transformations, decisions, and evidence rather than through model output or final-user conduct alone.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 29 Aug 2025

Revised: 26 Sep 2025

Accepted: 09 Nov 2025

Published online: 25 May 2026

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

- Klerkx L, Jakku E, Labarthe P. A review of social science on digital agriculture, smart farming and agriculture 4.0: New contributions and a future research agenda. *NJAS Wagening J Life Sci*. 2019;90-91:100315.
<https://doi.org/10.1016/j.njas.2019.100315>.
- Gwagwa A, Kazim E, Kachidza P, Hilliard A, Siminyu K, Smith M, et al. Road map for research on responsible artificial intelligence for development (AI4D) in African countries: The case study of agriculture. *Patterns*. 2021;2(12):100381.
<https://doi.org/10.1016/j.patter.2021.100381>.
- Dara R, Hazrati Fard SM, Kaur J. Recommendations for ethical and responsible use of artificial intelligence in digital agriculture. *Front Artif Intell*. 2022;5:884192.
<https://doi.org/10.3389/frai.2022.884192>.
- Ryan M. The social and ethical impacts of artificial intelligence in agriculture: Mapping the agricultural AI literature. *AI Soc*. 2023;38(6):2473-85.
<https://doi.org/10.1007/s00146-021-01377-9>.

Alexander CS, Yarborough M, Smith A. Who is responsible for 'responsible AI'? Navigating challenges to build trust in AI agriculture and food system technology. *Precis Agric.* 2024;25(1):146-85.
<https://doi.org/10.1007/s11119-023-10063-3>.

Mallinger K, Baeza-Yates R. Responsible AI in farming: A multi-criteria framework for sustainable technology design. *Appl Sci.* 2024;14(1):437.
<https://doi.org/10.3390/app14010437>.

Gardezi M, Adereti DT, Stock R, Ogunyiola A. In pursuit of responsible innovation for precision agriculture technologies. *J Responsible Innov.* 2022;9(2):224-47.
<https://doi.org/10.1080/23299460.2022.2071668>.

Bronson K. Looking through a responsible innovation lens at uneven engagements with digital farming. *NJAS Wagening J Life Sci.* 2019;90-91:100294.
<https://doi.org/10.1016/j.njas.2019.03.001>.

Wiseman L, Sanderson J, Zhang A, Jakku E. Farmers and their data: An examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming. *NJAS Wagening J Life Sci.* 2019;90-91:100301.
<https://doi.org/10.1016/j.njas.2019.04.007>.

Jakku E, Taylor B, Fleming A, Mason C, Fielke S, Sounness C, et al. "If they don't tell us what they do with it, why would we trust them?" Trust, transparency and benefit-sharing in smart farming. *NJAS Wagening J Life Sci.* 2019;90-91:100285.
<https://doi.org/10.1016/j.njas.2018.11.002>.

Atik C. Towards comprehensive European agricultural data governance: Moving beyond the "data ownership" debate. *IIC Int Rev Intellect Prop Compet Law.* 2022;53(5):701-42.
<https://doi.org/10.1007/s40319-022-01191-w>.

Ryo M. Explainable artificial intelligence and interpretable machine learning for agricultural data analysis. *Artif Intell Agric.* 2022;6:257-65.
<https://doi.org/10.1016/j.aiia.2022.11.003>.

Eastwood C, Ayre M, Nettle R, Dela Rue B. Making sense in the cloud: Farm advisory services in a smart farming future. *NJAS Wagening J Life Sci.* 2019;90-91:100298.
<https://doi.org/10.1016/j.njas.2019.04.004>.

Fielke S, Taylor B, Jakku E. Digitalisation of agricultural knowledge and advice networks: A state-of-the-art review. *Agric Syst.* 2020;180:102763.
<https://doi.org/10.1016/j.agsy.2019.102763>.

Carolan M. Acting like an algorithm: Digital farming platforms and the trajectories they (need not) lock-in. *Agric Hum Values.* 2020;37(4):1041-53.
<https://doi.org/10.1007/s10460-020-10032-w>.

Ruder SL. The 'terms and conditions' of surveillance capitalism: Theorizing agricultural data policy and governance. *J Peasant Stud.* 2025;52(4):725-50.
<https://doi.org/10.1080/03066150.2024.2429480>.

Sparrow R, Howard M. Robots in agriculture: Prospects, impacts, ethics, and policy. *Precis Agric.* 2021;22(3):818-33.
<https://doi.org/10.1007/s11119-020-09757-9>.

Eastwood CR, Dela Rue B, Edwards JP, Jago J. Responsible robotics design—a systems approach to developing design guides for robotics in pasture-grazed dairy farming. *Front Robot AI.* 2022;9:914850.
<https://doi.org/10.3389/frobt.2022.914850>.

Ryan M, van der Burg S, Bogaardt MJ. Identifying key ethical debates for autonomous robots in agri-food: A research agenda. *AI Ethics*. 2022;2(3):493-507.

<https://doi.org/10.1007/s43681-021-00104-w>.

van der Burg S, Giesbers E, Bogaardt MJ, Ouweltjes W, Lokhorst K. Ethical aspects of AI robots for agri-food; a relational approach based on four case studies. *AI Soc*. 2024;39(2):541-55.

<https://doi.org/10.1007/s00146-022-01429-8>.

Aby GR, Issa SF. Safety of automated agricultural machineries: A systematic literature review. *Safety*. 2023;9(1):13.

<https://doi.org/10.3390/safety9010013>.

van der Burg S, Bogaardt MJ, Wolfert S. Ethics of smart farming: Current questions and directions for responsible innovation towards the future. *NJAS Wagening J Life Sci*. 2019;90-91:100289.

<https://doi.org/10.1016/j.njas.2019.01.001>.

Rotz S, Duncan E, Small M, Botschner J, Dara R, Mosby I, et al. The politics of digital agricultural technologies: A preliminary review. *Sociol Ruralis*. 2019;59(2):203-29.

<https://doi.org/10.1111/soru.12233>.

Rose DC, Chilvers J. Agriculture 4.0: Broadening responsible innovation in an era of smart farming. *Front Sustain Food Syst*. 2018;2:87.

<https://doi.org/10.3389/fsufs.2018.00087>.

Amiri-Zarandi M, Dara RA, Duncan E, Fraser EDG. Big data privacy in smart farming: A review. *Sustainability*. 2022;14(15):9120.

<https://doi.org/10.3390/su14159120>.

Novelli C, Taddeo M, Floridi L. Accountability in artificial intelligence: What it is and how it works. *AI Soc*. 2024;39(4):1871-82.

<https://doi.org/10.1007/s00146-023-01635-y>.

Busuioc M. Accountable artificial intelligence: Holding algorithms to account. *Public Adm Rev*. 2021;81(5):825-36.

<https://doi.org/10.1111/puar.13293>.

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. *Sci Eng Ethics*. 2020;26(4):2141-68.

<https://doi.org/10.1007/s11948-019-00165-5>.

Floridi L, Cowls J, Beltrametti M, Chatila R, Chazerand P, Dignum V, et al. AI4People—an ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds Mach*. 2018;28(4):689-707.

<https://doi.org/10.1007/s11023-018-9482-5>.

Martin K. Ethical implications and accountability of algorithms. *J Bus Ethics*. 2019;160(4):835-50.

<https://doi.org/10.1007/s10551-018-3921-3>.