World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

HUMAN-CENTERED COMPLIANCE ANALYTICS: BUILDING TRANSPARENT DATA GOVERNANCE MODELS FOR CUSTOMER-FOCUSED DIGITAL PLATFORMS

Anjali Kansara *

Dallas Baptist University
* Corresponding Author

ORCID Details
Anjali Kansara: https://orcid.org/0009-0009-3267-6420

World Journal of Advanced Engineering Technology and Sciences, 2026, 21(02), 041–052

Publication history: Received on 04 August 2026; revised on 02 November 2026; accepted on 04 November 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.21.2.0453

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

The rapid expansion of customer-focused digital platforms has increased the complexity of managing regulatory compliance, personal data, privacy requirements, and customer expectations for transparency. Conventional compliance analytics primarily emphasize organizational risk detection and regulatory reporting, often providing limited visibility into how customer data is collected, processed, shared, and governed. This paper proposes a human-centered compliance analytics framework that integrates transparent data governance, continuous compliance monitoring, explainable analytics, and human oversight within customer-oriented digital environments. The proposed approach connects data lifecycle management with policy enforcement, risk identification, auditability, and customer-facing transparency mechanisms. It emphasizes data lineage, consent management, explainable compliance decisions, accountability, and customer agency as core governance dimensions. The framework further introduces measurable evaluation criteria for compliance effectiveness, transparency, explainability, responsiveness, and customer trust. By shifting compliance from a predominantly control-oriented function to a transparent, participatory governance model, the study shows how analytics can support both regulatory accountability and customer confidence. The proposed framework provides organizations with a structured foundation for designing adaptive, explainable, and customer-focused compliance capabilities across digitally enabled service ecosystems.

Keywords: Human-Centered Compliance, Compliance Analytics, Data Governance, Explainable Analytics, Customer Trust.

1 INTRODUCTION

Digital platforms have revolutionized how customers interact with organizations, weaving data collection, analysis, personalization, automated decision-making, and continuous service delivery into the digital experience. On the customer side, platforms are becoming more personal and understanding, using personal, behavioral, transactional, and contextual data to better understand users, enhance services, identify risks, and offer personalised interactions [1]. In this sense, data governance is no longer database administration or regulatory record-keeping, but a policy, technical

control, responsibilities, and accountability during the entire lifecycle of data - from the moment it is taken, when it is processed and shared for end-to-end use, all the way to the moment of retention and, since then, the data is deleted. Thus, smart governance mechanisms must balance the value that can be gleaned from data use with the need to respect privacy, security, transparency, customer empowerment, and compliance with rules [2]. For instance, the NIST Privacy Framework is an organization's capability to maintain individuals' privacy and security without losing innovative products and services. Likewise, current data-governance principles are limited because they must reconcile data access and reusability with privacy, trust, conflicting stakeholder interests, and individual empowerment [3]. Compliance Analytics is the analytical part of compliance, so it can continually audit data-processing activities, detect non-alignment incidents, assess compliance likelihood, review controls, and produce evidence of compliance for accountability. Compliance on its own, however, cannot be guaranteed because of the good performance of an internal control. The customer's perception of meaningful compliance also requires information, for example, of what information exists, why the data is processed and how decisions are taken, as well as options and remedies for the customer. Transparency thus plays an inherent role in trustworthy digital governance. There are a number of studies that have identified that transparency reporting is happening; however, some of the information provided has been identified as not having enough 'informative value' [4], or it fails to be comparable, or there is a disconnect between what actually is provided and what is known about the criteria for transparency reporting [5]. This has shifted emphasis to human-centric compliance analytics, with the customer's right, expectation, understanding, or control at the centre of compliance.

Principles of data governance are not the same as data being governed, and when the gap between privacy practice improvements is so vast, data governance challenges keep increasing. Some progress has been made in privacy management and data governance, including accountability and automation for privacy compliance monitoring through algorithms, but the disconnect between governance principles and how data is governed remains vast. Traditionally, these functions operate through separate processes and distinct governance structures, resulting in inconsistent synchronization of customer consent data and fragmented sharing of regulatory compliance information across systems. Although data-governance strategies and objectives are well established, challenges remain in translating them into effective operational practices [5]. Additional limitations persist in data-quality management, interoperability, and systematically measuring governance impact. Recent experiences across OECD countries further highlight these implementation gaps. For now, compliance analytics is less about educating and engaging customers on the processes that use and generate data and more about the organization's risk and the effectiveness of regulatory reporting and risk management. With the rise of automated profiling and automated decisions in digital services, this limitation becomes particularly relevant. The GDPR provides specific protections against automated decisions, including situations where human intervention is needed and there is an opportunity to provide a viewpoint or contest a decision [6]. Similarly, AI systems must be recorded and have "good human oversight" for higher-risk systems under new AI regulations [7]. Transparency, however, is not easily achieved, because providing more information doesn't necessarily lead to understanding or to trust. However, recent work suggests that, depending on the user, their characteristics, and how information is presented, transparency can affect trust differently [8]. The crucial research gap in this context is how to integrate compliance Analytics with human-centered governance mechanisms that can frame compliance events as meaningful, traceable, and actionable information for Customer Users. Explainability, customer agency, human supervision, and measurable transparency are crucial components that must be central to the complete model to meet regulatory requirements and internal analysis needs.

This paper addresses these challenges by proposing a Human-Centered Compliance Analytics framework to enhance transparency in data governance across customer journeys and digital platforms. Rather than functioning solely as an internal control mechanism or periodic audit process, the proposed model establishes compliance analytics as a continuous governance capability. It provides an integrating layer across key governance functions, including data lifecycle management, analytical oversight, explainability, accountability, and customer interactions. The framework covers identifying, evaluating, explaining, escalating, and communicating compliance events without losing human and customer control. It also provides measurable indicators, or yardsticks, for governance based on factors beyond compliance. The study is therefore confined to the following scope:

- Create a compliance analytics framework focused on the human aspects and regulatory controls, data governance, data analytics, and transparency for customers.
- Set up and clarify a clear Data Governance framework for Data Lifecycle Management, Data Lineage, Data Consent (Data Culture), Data Access, Data Retention, and Data Accountability.
- Inherit explainability and human control in an automated compliance monitoring and decision-making process.
- Create transparency, compliance effectiveness, explainability, and responsiveness as customer-oriented metrics to be evaluated, as well as customer agency.
- Explain the principles behind the governance of reliable and trusted digital platforms, with reference to the potential governance models and related impact of a digital platform.

2 RELATED WORK

Algorithmic accountability, transparency, and trustworthy analytics have evolved from "stand-alone" technical solutions to Data Governance models. Studies stated that one foundation of trusted AI is data governance, highlighting stewardship, risk-based governance, and controlled scrutiny and accountability of data algorithms throughout their lifecycle [9]. Previous governance studies also emphasized the need for system checks to reduce opacity, improve accountability, and, notably, mitigate automation effects [10]. Other studies have confirmed the relationship between transparency and platform governance, suggesting that transparency mechanisms can support platform governance even in contexts where traditional enforcement is weak [11]. Research on GDPR accountability also suggests that accountability goes beyond transparency and needs to include governance systems and human responsibility [12]. Later, such theorists proposed involving stakeholders from the targeted population in explaining algorithms and regulatory requirements [13] and began to "governmentalize" the technical elements of explainability. User characteristics and algorithmic literacy have also been part of empirical research, as they affect transparency towards users of algorithms [14]. Platform research is a developing area that can reveal platforms that restrict access to key information needed for an algorithmic audit, creating further challenges for independent scrutiny [15]. Automated transparency measures have also been explored in recent research, which has revealed that transparency disclosure does not necessarily lead to uniformity and meaningful transparency [16]. Newer research on data-governance transparency aims to evaluate the transparency of user assessments, focusing on understandability, predictability, accountability, and recourse [17]. Together, these highlight the need to reconsider governance as a more proactive, explainable, and customer-focused approach, and to incorporate compliance analytics with data lifecycle governance, a human touch, and customer focus and visibility.

The field has increasingly morphed from the traditional data-governance and algorithmic-accountability hydra to the predictive, high-level discipline of transparency, explainability, stakeholder engagement, and automated governance, as highlighted by the studies summarized in Table I. Effective management of data, processes, and algorithms is crucial for trustworthy AI [9], and opacity and lack of accountability are among the challenges highlighted by the European framework with regard to algorithmic decision-making [10]. Regarding their potential to emerge, platform research analysis shows that transparency is a means of governance itself, while under GDPR transparency is approached through the lens of accountability and human accountability. This is supported by a stakeholder-centric approach, which highlights the need to design transparency mechanisms that respond to the needs of affected stakeholders [13]. Two realms of empirical research offer further insights into issues around explainability and user manipulation and control, indicating that accounting for how users actually use and interpret algorithmic systems affects transparency [14]. In practice, some newer platform studies highlight issues of independent auditing and transparency [15, 16], and new research on data governance increasingly links transparency to users' understanding, trust, and recourse [17]. Several studies showed the feasibility of continuous, AI-enabled automated governance approaches in most case studies. As shown in Table I, however, most research to date focuses on these dimensions alone. Human understanding of compliance data and data lifecycle governance remains a major research challenge and has not yet been integrated into a single "human-centric" model that includes compliance analytics, explainability, oversight, and customer transparency. This study's proposed framework addresses this gap.

Table 1: Related Work on Compliance Analytics, Data Governance, and Transparency

Ref.	Core Contribution	Approach / Key Elements	Relevance to Present Study	Identified Limitation / Remaining Gap
[9]	Established data governance as a foundation for trustworthy AI and algorithmic systems.	Data stewardship, risk-based governance, system-level controls, trusted information sharing, accountability.	Provides the governance foundation for integrating data, algorithms, and compliance controls.	Primarily focuses on organizational and system governance rather than customer-facing compliance transparency.
[10]	Examined governance challenges arising from opaque algorithmic decision-making.	Transparency, accountability, regulatory oversight, awareness, liability, and institutional governance.	Supports the need for transparent and accountable automated decision-making.	Does not provide an integrated analytics architecture connecting compliance events with customer interaction.
[11]	Demonstrated how transparency can function as a governance	Platform transparency, external observation, legitimacy assessment, machine-learning-supported classification.	Establishes transparency as an operational governance instrument rather than	Focuses on platform-level legitimacy and does not comprehensively address customer data lifecycle governance.

	mechanism within digital platforms.		merely a disclosure requirement.	
[12]	Emphasized accountability and human responsibility within algorithmic governance.	GDPR principles, accountability, human involvement, systematic governance processes.	Reinforces the importance of human oversight and accountable compliance processes.	Provides primarily a regulatory and conceptual perspective rather than an analytics-driven implementation model.
[13]	Proposed a stakeholder-oriented approach to designing transparent, regulatory-compliant systems.	Stakeholder identification, explainability, human-centered computing, transparency, regulatory compliance.	Directly supports the human-centered orientation of the proposed framework.	Focuses mainly on algorithmic transparency and does not fully integrate enterprise data governance and continuous compliance analytics.
[14]	Investigated the relationship between explainability, user control, and perceived transparency.	User studies examining explainability, control, transparency, and algorithmic literacy.	Supports incorporating user control and understandable explanations into compliance governance.	User perceptions are examined more strongly than organizational compliance workflows and governance architecture.
[15]	Identified an accountability gap created when platforms restrict access required for independent algorithmic oversight.	Comparative platform analysis, audit access, transparency mandates, independent verification.	Demonstrates the practical difficulty of achieving meaningful external accountability in platform environments.	Concentrates on platform auditing and access rather than customer-level data governance and compliance analytics.
[16]	Evaluated automated transparency mechanisms used by online platforms.	Large-scale transparency database analysis, platform disclosures, statements of reasons, compliance evaluation.	Shows how automated reporting can support regulatory transparency while enabling empirical compliance analysis.	Formal transparency mechanisms can still leave substantial discretion and variation in actual platform practices.
[17]	Developed a user-oriented view of perceived data-governance transparency.	Understandability, predictability, accountability, data-use transparency, trust, user recourse.	Directly connects governance transparency with users' perceptions and trust.	Highlights the importance of user perception but does not establish a complete compliance analytics architecture.
[18]	Explored AI-supported approaches for real-time and automated data governance.	Event-driven governance, automated data classification, intelligent policy enforcement, proactive monitoring.	Supports the transition from manual compliance workflows toward continuous, analytics-enabled governance.	Automation can improve governance efficiency but requires stronger human-centered explanations, accountability, and customer-facing transparency.

3 PROPOSED HUMAN-CENTERED COMPLIANCE ANALYTICS ARCHITECTURE

The proposed architecture positions compliance as a constant, person-centric capability, and not an audit function. It is designed to help address the need to link the four components of data governance, regulatory controls, analytics, transparency, and customer agency into a single operational framework. In today's context, effective governance research focuses more on coordination, accountability, interoperability, and ongoing data governance, rather than simply having data controls. More recent multi-layer governance architectures also confirm the principles and importance of aggregating data assessment, policy management, analytics, controls, interoperability, and continuous feedback loops. The proposed architecture explicitly incorporates the customer as a stakeholder in compliance governance, while securely interweaving compliance analytics with explainability and direct human oversight. The architecture consists of 5 connected layers: Customer Interaction and Agency; Data Governance and Lifecycle Management; Compliance Analytics and Risk Intelligence; Explainability and Human Oversight; Audit, Feedback and

Continuous Improvement. Data and compliance events flow upward through the architecture for classification, analysis, risk assessment, and decision support. In contrast, governance policies, human decisions, and customer preferences flow downward to guide and inform operational controls. The bidirectional flow prevents a 'one-way' compliance practice. Instead, it forms a feedback-driven governance cycle, so customer preferences, policy changes, analysis observations, evidence from human judgements, and audit evidence continually influence the next set of governance decisions. The design also embraces the principle of "privacy-by-design", key to trusted data governance, which limits the purpose of data processing, requires explicit consent, minimizes data collected, exercises data retention control, and maintains an audit trail of data processing. The architecture thus aims to achieve three outcomes: compliance, accountability, and meaningful customer control. Changes in compliance position can be identified, communicated, recorded, reviewed, and explained through shared governance and analytics processes to create transparency in digital-platform operations, making compliance easy to track, explain, review, record, and communicate throughout the data lifecycle.

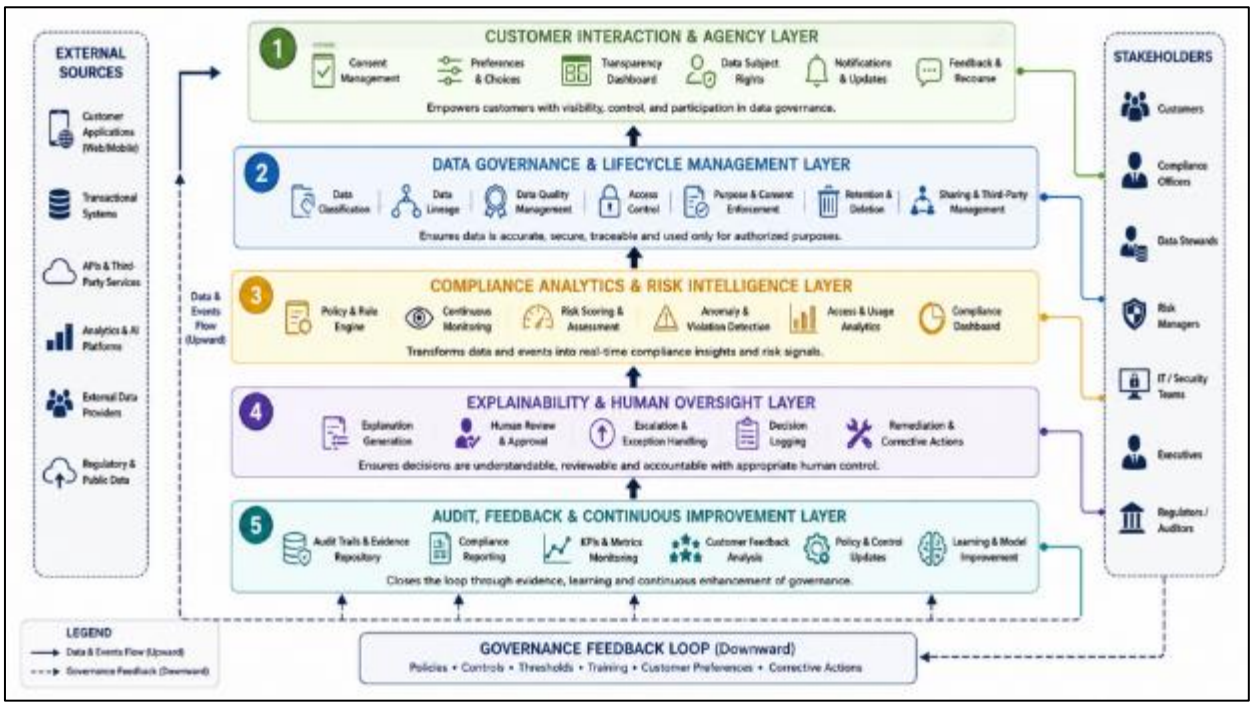


Figure 1: Proposed Human-Centered Compliance Analytics Architecture

3.1 Customer Interaction and Agency Layer

Compliance mechanisms should protect and support the individuals whose data is being processed. Accordingly, the proposed architecture incorporates a people-centered Customer Interaction and Agency Layer. Conventional compliance architectures, however, often focus primarily on providing information to customers while offering limited ability to influence or control how their data is subsequently used. The proposed approach shifts customers from passive recipients of information to active participants in data governance. It provides greater visibility into how their data is processed while enabling them to provide, modify, or withdraw consent when necessary. This approach also helps customers understand data practices, express their preferences, and exercise their data rights. Consent should therefore be granular, revocable, auditable, and linked to clearly defined purpose limitations rather than treated as a one-time decision. This layer stores the customer's preferences, with governance sending signals about how downstream layers should process and access the customer's data. A customer-oriented interface may reveal what categories of data are collected, why it is processed, how long it is held, who the third parties are, whether it is processed automatically, and what controls are available. The layer may also provide a way to communicate clearly about important changes, e.g., a change in the layer's data-processing purpose or a significant change to a policy. Most importantly, it is not viewed simply as a privacy notice and notification. The approach extends beyond conventional privacy notices and notifications. The architectural objective is to establish “usable transparency,” ensuring that relevant information and clear explanations are presented at an appropriate level for customers to understand and act upon. The layer can also provide feedback and recourse, allowing customers to question, correct, or challenge relevant governance outcomes. Such mechanisms strengthen the link between compliance and customer trust, and provide additional input into the corporate governance process. In this architecture, customer input becomes part of the governance information captured in the Consent process, feeds into Policy enforcement, highlights risk, and enables continuous improvement.

3.2 Data Governance and Lifecycle Management Layer

The Data Governance and Lifecycle Management Layer defines how customer data is governed throughout its lifecycle. It integrates key functions such as data discovery and classification, stewardship, lineage tracking, quality management, access control, purpose limitation, retention, and data sharing within a unified governance structure. This layer gets data from customer interactions with the app, transaction systems, analytics platforms, APIs, and data sources outside the organization. Metadata associated with each data asset captures key information, including data sensitivity, ownership, processing purpose, permitted uses, applicable policies, retention requirements, and lineage. This enables a traceable relationship between individual data elements and the governance rules that apply to them. Such traceability is particularly important in modern digital environments, where customer data is distributed across multiple applications, systems, and institutions. The requirements of cross-cutting data-platform functions, such as provenance, rights, consent, governance, and security, are also critical in modern data-platform architectures. The layer also includes built-in classification features to discover private, sensitive, regulated, and high-risk data and apply the appropriate level of data governance. But even though automation is supposed to end human stewardship, ambiguous classification may still require Data Stewards to review and confirm its accuracy. This layer adds lifecycle controls for collection, processing, storage, sharing, archival, and deletion. Data purpose limitation and data minimisation mechanisms can prevent data reuse for uses for which they are not specifically authorised, while data deletion controls rely on user deletion and, at the appropriate time, wiping the data and other data uses. Records of data lineage include information an organization might need to determine the origin of that data, how it was manipulated, the systems the data has traversed, and the conformity policies applicable to each system to which the data has been subjected. This layer translates and transforms abstract governance requirements into operational metadata and controls that drive compliance analytics.

3.3 Compliance Analytics and Risk Intelligence Layer

CARIL transforms actionable information and data into ongoing compliance intelligence. Continually monitors processing activities to conform to those required by organizational policies, controls, and regulatory procedures, consent conditions, and predetermined risk thresholds, without having to wait for an audit. The analytics components include rule-based compliance checks, anomaly detection, risk scoring, policy-to-data matching, access-pattern analysis, retention monitoring, consent validation, and violation detection. For each major processing event, three reviews can be conducted (before, during, and after), based on specific governance requirements and the event's risk and operational needs. For instance, a data-sharing event can be evaluated based on the degree of privacy involved, the purpose of sharing, and even the audience(s), their existing knowledge of the event, their experience with the event, etc. This analysis can yield a compliance risk score, which could trigger automatic activation of further controls, or the scores could be passed to human review systems. Recent governance research highlights the value of dynamic, risk-aware architectures. In such environments, governance mechanisms continuously assess emerging risks and adapt controls in response to changing conditions. Similarly, new governance platforms that attempt to actively control events are moving from manual event classification to policies enforced on events. However, the key point of the proposed model is that analytics are never perceived as making decisions on their own. Low-value events pass through predetermined automated controls, while higher-significance or more complex events are escalated to human oversight. The layer also captures a wealth of compliance context, such as triggering information, the policy to apply, data classification, risk-score evaluation, the decision outcome, and the control action applied. This evidence is crucial for later explaining, auditing, and remediating. Compliance analytics is the analytical engine, plugged into real-time activity from any operation and actions that derive from any governance.

3.4 Explainability and Human Oversight Layer

The Explainability and Human Oversight Layer aims to make compliance decisions made by analytical and automated processes explainable, reviewable, and accountable. A key limitation of automated compliance systems is their inability to adequately explain why an activity is classified as non-compliant or provide sufficient evidence to support the determination. The proposed layer addresses this limitation by introducing an explainable compliance framework. It links compliance outcomes to the relevant data, policies, risk assessments, and corresponding control responses. For example, a high-risk processing event could result from a data-type category, a processing use, a governing rule, a recognized deviation, risk factors, and suggested next steps. This will aid and simplify compliance officers, data stewards, auditors, and customers (where relevant). Explainability, traceability, auditability, and compliance are no longer treated as secondary considerations addressed only after a system has been developed. Instead, these principles are increasingly incorporated into the system architecture from the outset as fundamental design requirements. Human oversight is an element of governance and not just a ‘follow-up' mechanism. Authorized reviewers are asked to address extreme incidents, those with uncertain policy impacts, or those that may be very significant to customers. Reviewers can approve, disapprove, edit, and request further evidence before taking action. The layer also takes care of deviations, handles exceptions and remediation, not only documented, but assigned as well and followed up until it is done. Human actions provide an additional source of governance evidence and can be analyzed to refine policies and rules based on observed decisions and contextual requirements. Automation supports speed, consistency, and continuous monitoring,

while human involvement remains essential for exceptional cases and context-sensitive interpretation. This balance maintains human oversight in decision-making while leveraging automated governance capabilities. Consequently, explainability becomes an integral design requirement rather than merely a reporting function.

3.5 Audit, Feedback and Continuous Improvement Layer

The Audit, Feedback, and Continuous Improvement Layer strengthens the governance loop by transforming compliance activities and human decisions into continuous sources of evidence for evaluating performance and governance outcomes. It maintains secure and tamper-resistant audit records linked to relevant processing activities, policy versions, consent status, explanations, human interventions, exceptions, and remediation outcomes. Records support internal audit, regulatory examination, and incident reporting. The layer supports key governance performance indicators, including compliance detection rates, frequency of policy violations, average remediation time, explanation coverage, consent-conformance rates, unresolved exceptions, and trends in customer-related outcomes. Importantly, auditing is not treated as the final stage of the compliance process. Instead, audit findings are fed back into the governance framework to support continuous refinement of policies, controls, and overall governance design. Any further breaches will lead to policy amendments, modified analytical thresholds, additional controls and employee involvement, or a redesign of processes that include customers. Customer feedback may also help identify processes that are technically correct but confusing or difficult to implement. This allows a feedback (information) mechanism to influence controls and supports continuous governance, for example, because monitoring data can be used as a record of past actions or behaviors rather than to influence and shape controls. The layer also provides governance dashboards with different levels of visibility, based on the information needs of customers, compliance teams, executives, auditors, and regulators with specific roles. This role-based approach ensures the right information is provided for relevant governance without compromising transparency. The evidence gathered and organized will be standardized for recurring compliance issues, emerging risks, and gaps in compliance controls and governance that may impact the customer base. The final form will be a much more reactive compliance regime, whereby the proposed compliance regime becomes a continuous compliance learning regime, where learning and development take place in response to changes in compliance versus evolving compliance standards, developments and changes, and evolving consumer demands.

4 HUMAN-CENTERED COMPLIANCE ANALYTICS MECHANISMS

The presented human-centric compliance analytics approach is intended as a continuous system for detecting, assessing, describing, and solving compliance challenges throughout the customer data lifecycle. While fundamental compliance systems generally involve periodic assessment and reporting against governance, policies, consent conditions, organizational control systems, and relevant parts of regulations, the proposed approach provides ongoing monitoring to identify mismatches. This process starts with events that could be identified as compliance-related, triggered by customer interactions, data access activities, data-sharing events, or preference changes. These events are classified by data sensitivity, data processing purpose, customer access, and the applicable data governance rules. Next, through policy rules, risk-scoring models, anomaly detection, and pattern analysis, the compliance analytics layer detects potentially excessive, inconsistent, anomalous, or unauthorized activity. Only some events are acted on, prioritized based on potential customer and regulatory impact. If high-risk or ambiguous events are encountered, they are sent to authorised human reviewers, while low-risk ones are covered by default controls. The explainability mechanism provides background on the detected event, such as references to the policy, data category, trigger condition, risk factors, and suggested mitigation actions. Human reviewers can validate the analytical result, approve or disapprove an action, request further evidence, or begin remediation. Therefore, amended decisions are recorded, creating a traceable record and continuing provision of governance feed-forward and back-loop. Customer-facing mechanisms then communicate, in comprehensible terms, about relevant data practices, consent changes, decisions, and remediation results. Information from customers and observed compliance is then fed into governance metrics and subsequent improvement processes. This establishes a closed-loop system comprising data events, analytical signals, governance decisions, customer-based actions, feedback, and better governance controls. It is mostly automated, with added human decision-making and the opportunity to trace and deliver customers' agency throughout the entire compliance process.

The mechanisms proposed do not work individually as compliance functions, but as an integrated “operational chain”, similar to the one shown in Table II. Then, continuous monitoring detects the first clue of an event, and classification and consent analytics establish the context in which the event is understood. Policy evaluation and risk scoring then determine whether an activity is a real or potential compliance issue and set its priority. Anomaly detection can identify unusual patterns that static rules may miss. However, analytical detection should not automatically determine the final governance decision. Instead, explainability and human-in-the-loop review provide an accountability bridge between automated analytics and consequential governance actions. This is particularly important in customer-facing platforms, where an analytically valid result may still require interpretation within the customer’s specific context before taking appropriate action. An exception-handling and recourse routine will minimise identified exceptions after validation,

rather than simply logging them. Last, audit and evidence generation will minimise decision-making during the process, while customer transparency mechanisms will transform relevant governance-outcome information into actionable insights for customers. Finally, customer feedback, compliance performance, and recurring risk patterns contribute to governance improvement. Together, these mechanisms establish a closed-loop compliance process encompassing detection, contextualization and assessment, explanation, human review, remediation, communication, and continuous learning. This iterative process enables the proposed governance model to translate human-centered governance principles into sustained and adaptive compliance practices.

Table 2: Human-Centered Compliance Analytics Mechanisms

Mechanism	Operational Function	Analytical / Governance Process	Human-Centered Outcome	Example Output
Continuous Compliance Monitoring	Continuously observes customer-data processing and system activities.	Compares real-time events against policies, permissions, consent conditions, and governance rules.	Reduces dependence on periodic audits and enables timely intervention.	Compliance alert or normal-event confirmation
Data Classification and Context Analysis	Determines the sensitivity and governance requirements of data involved in an event.	Classifies data according to personal, sensitive, regulated, transactional, or other categories and associates applicable policies.	Helps ensure that customer information receives proportionate protection.	Data-risk classification
Consent and Preference Analytics	Verifies whether processing is consistent with customer permissions and preferences.	Matches processing events with consent status, purpose, preference, and permitted-use conditions.	Strengthens customer control over data use.	Consent-compliance status
Policy and Rule Evaluation	Determines whether an activity complies with predefined governance requirements.	Applies policy rules to data events, access requests, sharing activities, retention actions, and other operations.	Makes governance requirements operational and consistently enforceable.	Policy pass/fail result
Risk Scoring and Prioritization	Assigns risk levels to detected compliance events.	Combines data sensitivity, event characteristics, policy violations, customer impact, and contextual risk indicators.	Directs human attention toward the most consequential cases.	Low, medium, or high-risk score
Anomaly and Violation Detection	Identifies unusual or potentially unauthorized behavior.	Uses statistical, rule-based, or machine-learning techniques to detect deviations from expected behavior.	Enables earlier identification of potentially harmful activities.	Anomaly alert
Explainable Compliance Decisions	Explains why an event was flagged or a decision was produced.	Links the outcome to the triggering event, applicable rule, evidence, and risk factors.	Improves understanding and reduces opaque compliance decisions.	Decision explanation
Human-in-the-Loop Review	Provides human validation for significant or ambiguous compliance events.	Escalates cases according to predefined risk thresholds and review requirements.	Preserves human accountability and contextual judgment.	Approval, rejection, or modified decision
Exception and Remediation Management	Handles confirmed violations and	Assigns responsibility, tracks corrective actions,	Provides accountability and a	Remediation case and resolution record

	governance exceptions.	and monitors resolution status.	path toward correction.	
Audit and Evidence Generation	Maintains evidence of compliance activities and decisions.	Records events, policies, decisions, explanations, interventions, and remediation actions.	Supports accountability, verification, and regulatory review.	Auditable compliance record
Customer Transparency and Feedback	Communicates relevant governance information to customers.	Converts internal compliance information into understandable explanations, notifications, dashboards, and feedback mechanisms.	Improves customer awareness, agency, and trust.	Transparency notification or customer feedback
Continuous Governance Improvement	Uses accumulated compliance and customer information to improve controls.	Analyzes recurring violations, false positives, customer feedback, and performance metrics to refine policies and analytical models.	Enables governance to adapt to changing risks and customer expectations.	Updated policy, threshold, or analytical model

5 IMPLEMENTATION AND EVALUATION FRAMEWORK

The proposed Human-Centered Compliance Analytics can be provided as a layered governance feature that is integrated into the digital-platform environment, not as a new digital-platform compliance system. The first step is to develop a comprehensive understanding of the customer data landscape. This includes identifying applications, transactional systems, APIs, analytics platforms, external data sources, and data storage locations. It also requires assessing data sensitivity, processing purposes, ownership, retention requirements, and applicable governance obligations. These governance policies are then translated into machine-readable, or even executable, concepts to evaluate against data-processing events. Metadata and lineage allow tracing individual data elements back to their data source, data use, data acceptance or rejection, permissions, and retention policies, and provide contextual data for compliance analytics to evaluate activities. These continuous monitoring mechanisms can be leveraged for compliance-relevant events like access, processing, sharing, retention, etc., via rule-based checks, anomaly detection, and risk scoring. Events can be escalated to Compliance Officers, Data Stewards (or other authorized reviewers) based on their Risk Thresholds. The explainability layer creates major event information, including the trigger event, the triggering policies, detected deviations, risk factors, and the proposed response. This is linked to the audit trail, and a human checks the analysis result and can confirm or correct it. Use options, if applicable, can then be offered to customers with consent controls, privacy dashboards, notices about the use of information, and explanations about information usage, without requiring more information than the law requires. Finally, audit evidence, human review outcomes, and customer feedback feed into the governance feedback loop to refine policies, controls, and analytical models as needed. These implementation elements illustrate a potential pathway from conceptual architecture to operational practice rather than prescribing deployment within any specific organization. As a conceptual study, the framework provides a structured approach for integrating compliance analytics into existing data-governance and customer-experience capabilities.

The assessment against the evaluation framework occurs at the level of organizational compliance performance and customer-oriented governance outcomes. Evaluation is structured as a real evaluation model and a concept-based evaluation, and can also be used as a case study (case study evaluation) and an expert evaluation. As part of the framework, we consider five dimensions: compliance effectiveness, transparency, explainability, human accountability, and customer agency. Compliance effectiveness is the ability to identify compliance breaches and policy non-compliance, assess risks, prioritize them, and take action within required timelines. Transparency measures the ability to explain and track relevant data-processing and governance activities in a comprehensible way. This is part of a systems approach to explaining relationships between analytical compliance outcomes and root components, rules, evidence, and risk factors. Human Accountability assesses the preparedness and effectiveness of escalation, review, exception handling, and remediation processes. Customer agency involves not only customer visibility but also control, feedback, and a means of recourse. Additional supporting metrics include violations detected, compliance response time and explanation coverage, consent-conformance rate, exception rate, and audit completeness and resolution rate of customer feedback. Together, these dimensions show that the framework is examined through the lens of the existence of compliance controls and through the lens of compliance controls that are (in a specific language sense) understandable, accountable, and customer-oriented.

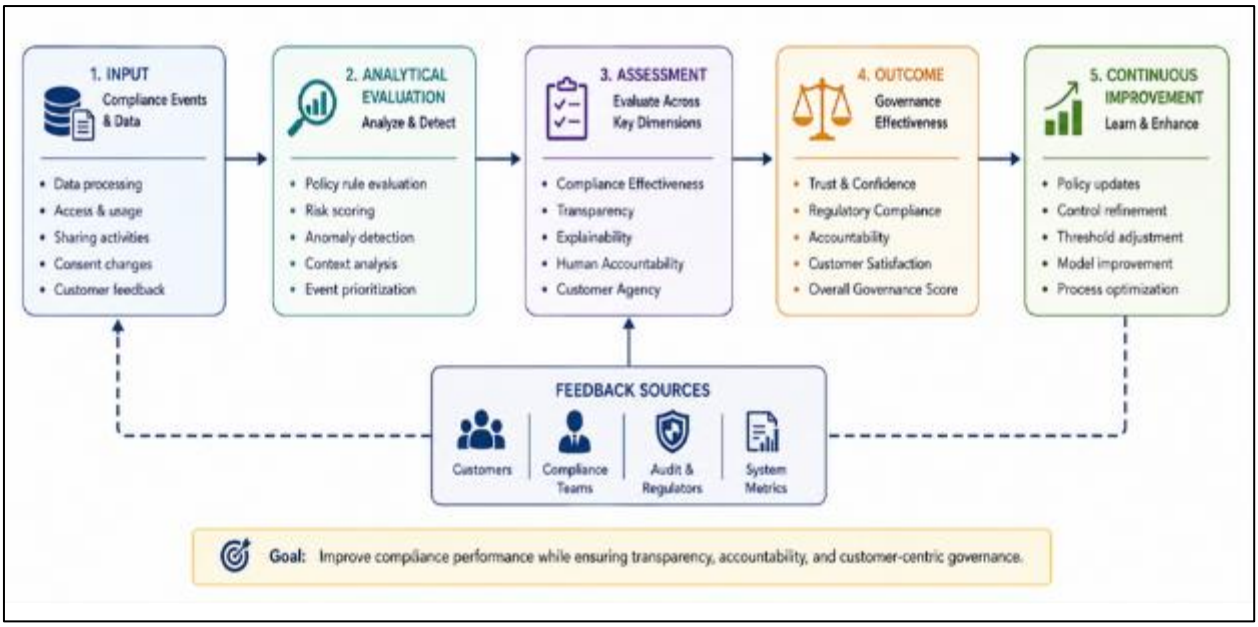


Figure 2: Evaluation Framework for the Proposed Human-Centered Compliance Analytics Model

LIMITATIONS

Customer-driven Digital Platforms cannot fully adhere to the Human-Centered Compliance Analytics framework, and applying Gauged Applications has limitations. A crucial factor in the framework's effectiveness is the quality, completeness, consistency, and timeliness of organizational data. Data lineage and compliance become tricky across a disjointed digital landscape, as customers and their data may be held in a variety of legacy applications, cloud services, APIs, third-party solutions, and departmental repositories. When tags are uninformative or poorly categorized, policies may be misapplied, and notes about non-compliance or alert counts may be excessive. Second, it also implies that a single governance mechanism cannot replace each set of regulations, as policies must be customized to specific situations. Regulatory changes could create additional needs for governance rules, analytical models, or compliance control updates. Third, AI systems used to automate anomaly detection and risk-scoring algorithms can generate false detections and miss compliance risks because behavioral patterns change or new and emerging risks are not present in the historical data. Excessive alerts may lead to alert fatigue, reducing users' attention and confidence in the monitoring system when notifications are perceived as irrelevant or low priority. Explainability adds another challenge, as outputs from complex analytical models may not always be sufficiently clear or interpretable for customers and operational teams. Reliable explanations will not cover all the technical and regulatory aspects that have been simplified. Fifth, when large numbers of high-risk events must be reviewed manually, human oversight can be delayed, which is not ideal, especially if an organization has insufficient compliance resources. Equally, organizations must balance transparency and privacy; revealing Governance information could expose confidential details about security, operations, and personal information. Furthermore, customers may engage with transparency mechanisms in different ways. Some may overlook privacy-related information, while others may find technical explanations difficult to understand or face challenges when exercising available data rights. Addressing these limitations requires robust data-quality assurance, clear mapping of regulatory requirements, appropriate human-resource capabilities, rigorous model validation, strong privacy safeguards, and effective communication practices.

FUTURE RESEARCH

Potential areas for further research include the proposed Human-Centred Compliance Analytics framework in relation to different kinds of customer-centred digital platforms and regulatory environments in different data-processing contexts. One such direction is creating adaptive compliance analytics that can translate future regulatory changes into governance policies, analytics rules, thresholds, and controls. This process may reduce manual work when updating compliance activities in response to regulatory changes. Compliance analytics approaches based on XAI techniques can also be explored further, focusing on using XAI to create explanations that are accurate, interpretable, contextually appropriate, and accessible for various parties. Other techniques offer similar promise, including privacy-preserving analytics (e.g., federated learning, secure computation) and others that can enable compliance monitoring without unnecessarily exposing customer information. Further research is needed to examine how compliance actions and customer feedback influence governance practices. Particular attention should be given to whether greater transparency, meaningful consent controls, and clear explanations strengthen customer trust and perceptions of fairness. Future studies should also investigate how these factors influence subsequent customer engagement with digital platforms. Empirical work with organizations and users would enable us to establish measurable links between

the user-friendliness of governance and performance in terms of compliance, incident prevention, satisfaction, and customer retention. Further comparative studies could examine how governance requirements vary across sectors, including financial services, healthcare, retail, telecommunications, hospitality, and other data-intensive industries. Such research could help determine how governance frameworks should be adapted to different regulatory and operational environments. Future studies could also explore autonomous or semi-autonomous compliance agents that continuously monitor compliance, identify potential issues, and recommend remediation measures. Particular attention should be given to maintaining appropriate human oversight and accountability over governance decisions. Another is fairness and bias detection, which could be extended from whether a rule has been violated to whether groups of customers are affected differently. Finally, longitudinal studies could explore how governance effectiveness unfolds as organizations build compliance paper trails, develop analytical models, incorporate customer feedback, and adapt to regulators' changing needs. These instructions can additionally tie up the dots among compliance engineering, responsible information management, Customer agency, and Digital trust.

6 CONCLUSION

Financial, personal, behavioral, transactional, and contextual data constantly challenge the management and monitoring of a digital platform as reporting expectations and demands increase. This paper explored key challenges in organizational controls, regulatory reporting and technical monitoring, and limited understanding of the customer, agency, and transparency. The Human-Centered Compliance Analytics framework extends these principles and further advances how these aspects can be brought together in a single framework that enables better customer interaction, data governance, compliance analytics, explainability, human compliance oversight, and continuous improvement. By using the architecture to correlate data lifecycle activities with policy evaluations, risk assessments, anomaly detection, consent validation, and compliance monitoring, they can leverage a clear path to document explanations, review, and corrective action for key and significant findings during data analysis. The framework also gives consumers awareness of the data assembly process, choice and preference, feedback, and the right to complain. The Data Capabilities for Resilient Digital Platforms outlined in the proposed implementation approach are intended to be implemented through various methods: controlling data classification, managing data lineage, enforcing policies, continuous monitoring, risk prioritization, human data review, generating audit evidence, and governance feedback. The evaluation framework focused on compliance effectiveness is a new approach to compliance that introduces components of transparency, explainability, human accountability, and customer agency. Issues of data quality, regulatory differences, approximation of analysis, human explanations, transparency, and privacy remain, but the framework specifies actions to address them. The study is general, suggesting that compliance effectiveness in the digital dimension can be assessed not only by compliance with regulatory requirements. It should also be evaluated for transparency, understandability, traceability, accountability, and responsiveness to customer needs, which will further strengthen the governance of digital platforms built on trustworthy principles.

REFERENCES

[1] ENTERPRISE, I. P. T. (2020). NIST privacy framework: a tool for improving privacy through enterprise risk management.

[2] Lefkovitz, N., & Boeckl, K. (2020). NIST privacy framework: An overview.

[3] Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly*, *37*(3), 101493.

[4] Urman, A., & Makhortykh, M. (2023). How transparent are transparency reports? Comparative analysis of transparency reporting across online platforms. *Telecommunications policy*, *47*(3), 102477.

[5] Llanos, J. (2021). Transparency Reporting: Considerations for the Review of the OECD Privacy Guidelines.

[6] Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *Regulation (EU)*, *679*(2016), 10-13.

[7] Union, E. (2024). Artificial Intelligence Act. *European Parliament: European Parliamentary Research Service*, *1689*, 2024.

[8] De Hert, P., & Lazcoz, G. (2022). When GDPR-principles blind each other: accountability, not transparency, at the heart of algorithmic governance. *Eur. Data Prot. L. Rev.*, *8*, 31.

[9] Kroll, J. A. (2015). *Accountable algorithms*. Princeton University.

[10] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big data & society*, *3*(2), 2053951716679679.

[11] Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *new media & society*, *20*(3), 973-989.

[12] James, A., Hynes, D., Whelan, A., Dreher, T., & Humphry, J. (2023). From access and transparency to refusal: Three responses to algorithmic governance. *Internet Policy Review*, *12*(2), 1-28.

[13] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, *7*(2), 76-99.

[14] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016, August). " Why should I trust you?" Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1135-1144).

[15] Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., ... & Gebru, T. (2019, January). Model cards for model reporting. In *Proceedings of the conference on fairness, accountability, and transparency* (pp. 220-229).

[16] Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe & trustworthy. *International Journal of Human-Computer Interaction*, *36*(6), 495-504.

[17] Tabassi, E. (2023). Artificial intelligence risk management framework (AI RMF 1.0).

[18] Smuha, N. A. (2025). Regulation 2024/1689 of the Eur. Parl. & Council of June 13, 2024 (EU Artificial Intelligence Act). *International Legal Materials*, *64*(5), 1234-1381.