

UNIVERSIDADE FEDERAL FLUMINENSE

IGOR GARCIA BALLHAUSEN SAMPAIO

A Reference Model for Data Driven Fraud Risk Analysis in Public Procurement

NITERÓI

2026

UNIVERSIDADE FEDERAL FLUMINENSE

IGOR GARCIA BALLHAUSEN SAMPAIO

A Reference Model for Data Driven Fraud Risk Analysis in Public Procurement

Thesis presented to the Computing Graduate Program of the Fluminense Federal University in fulfillment of the requirements for the degree of Doctor of Science. Field: Computer Science.

Advisor:

FLÁVIA CRISTINA BERNARDINI

Co-advisor:

JOSÉ VITERBO FILHO

NITERÓI

2026

Ficha catalográfica automática - SDC/BCPV
Gerada com informações fornecidas pelo autor

S192r Sampaio, Igor Garcia Ballhausen
A Reference Model for Data Driven Fraud Risk Analysis in
Public Procurement / Igor Garcia Ballhausen Sampaio. - 2026.
235 f.: il.

Orientador: Flávia Cristina Bernardini.
Coorientador: José Viterbo Filho.
Tese (doutorado)-Universidade Federal Fluminense, Instituto
de Computação, Niterói, 2026.

1. Governo Digital. 2. Dados Abertos Governamentais. 3.
Compras Públicas. 4. Produção intelectual. I. Bernardini,
Flávia Cristina, orientadora. II. Filho, José Viterbo,
coorientador. III. Universidade Federal Fluminense. Instituto
de Computação. IV. Título.

CDD - XXX

IGOR GARCIA BALLHAUSEN SAMPAIO

A Reference Model for Data Driven Fraud Risk Analysis in Public Procurement

Thesis presented to the Computing Graduate Program of the Fluminense Federal University in fulfillment of the requirements for the degree of Doctor of Science. Field: Computer Science

Approved in August, 2026.

APPROVED BY

D.Sc. Flávia Cristina Bernardini - Advisor, UFF

D.Sc. José Viterbo Filho - Co-advisor, UFF

D.Sc. Daniel Cardoso Moraes de Oliveira, UFF

D.Sc. Flávio Luiz Seixas, UFF

D.Sc. Nitesh Bharosa, TU Delft

D.Sc. Cristiano Maciel, UFMT

Niterói

2026

“On fait la science avec des faits, comme on fait une maison avec des pierres : mais une accumulation de faits n’est pas plus une science qu’un tas de pierres n’est une maison.”

Henri Poincaré

Acknowledgements

To my mother, who has always been my biggest supporter in my studies, who throughout much of my academic journey, never let me miss anything, trying her best to ensure that I could achieve all my professional and academic goals.

To my wife, for inspiring me with the topic of my thesis. Always understanding my choice and supporting me as I sacrificed days, nights, weekends and holidays to carry out this study.

To my family, for always being there, sharing laughter, encouraging me and celebrating my achievements. Your words of encouragement and pride have driven me at every stage of this journey.

To my friends, for the productive discussions, for the high-level debates and for knowing how arduous the process has been so far, believing in me from the beginning.

To the educational institution, for the environment conducive to learning and for the support offered throughout this academic journey. The academic excellence and commitment to teaching were fundamental to my personal and professional growth.

To my advisors, for their wise guidance, constant support and tireless encouragement. Your expertise, dedication and confidence in my potential were essential for the development of this work.

To my supervisors during my doctoral exchange at TU Delft, for their invaluable guidance, insightful discussions and for broadening my academic perspective in an international context. Your support during this period was fundamental to the maturation of this research.

To Franklin, the auditor from CGU, for his generosity in sharing knowledge, practical insights and for his continuous support throughout this journey. Your contributions were essential in bridging the gap between theory and real-world auditing practices.

I would like to thank all the people who interfered in my journey, as they influenced

it in some way.

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001.

Resumo

As Contratações Públicas (CP) representam uma parcela significativa dos gastos governamentais e permanecem altamente vulneráveis a fraudes, corrupção e outras irregularidades. Embora os avanços em Inteligência Artificial (IA) e Dados Governamentais Abertos (DGA) tenham criado novas oportunidades para apoiar atividades de fiscalização, os estudos existentes enfatizam predominantemente técnicas analíticas isoladas, negligenciando as condições mais amplas de dados, organizacionais, de governança e éticas necessárias para sua adoção eficaz na auditoria pública. Esta tese visa projetar e avaliar um modelo de referência para a análise de risco de fraude em CP orientada por dados, integrando perspectivas analíticas, sociotécnicas, de governança e éticas em uma abordagem unificada de apoio à decisão. Em vez de focar na detecção automatizada de fraudes, o modelo proposto auxilia auditores na identificação, priorização e investigação de indicadores de risco de fraude por meio de processos analíticos transparentes e responsáveis. A pesquisa segue o paradigma da Design Science Research, combinando revisões sistemáticas da literatura, entrevistas com especialistas, estudos empíricos quantitativos e qualitativos e a avaliação de artefatos. A pesquisa inclui: (i) uma avaliação comparativa dos ecossistemas de DGA de contratações públicas no Brasil, nos Países Baixos e na União Europeia, utilizando métricas quantitativas de qualidade de dados e análise sociotécnica; (ii) a construção de um catálogo de indicadores de risco de fraude apoiado por conjuntos de dados governamentais heterogêneos; (iii) o projeto de um modelo de referência em camadas, compreendendo as camadas de Dados, Motor Analítico, Decisão, Ética, Proveniência, Governança e Segurança, e Avaliação e Refinamento; e (iv) o desenvolvimento e a avaliação de um protótipo utilizando dados de contratações públicas brasileiras com auditores públicos. Os resultados demonstram que uma análise eficaz de risco de fraude depende não apenas de modelos de IA, mas também da disponibilidade de dados interoperáveis e de alta qualidade, de governança institucional, supervisão humana, explicabilidade, proveniência e mecanismos de avaliação contínua. A análise comparativa mostra, ainda, que a qualidade dos dados por si só não determina a capacidade analítica, a qual também emerge de condições legais, organizacionais e culturais que moldam os ecossistemas de dados de contratações públicas. O modelo de referência proposto foi avaliado positivamente por auditores públicos e demonstrou sua capacidade de apoiar a priorização e a interpretação de indicadores de risco de fraude, preservando a autoridade humana na tomada de decisões. Esta tese contribui para a pesquisa em Sistemas de Informação e Governo Digital ao fornecer um modelo de referência sociotécnico que integra infraestruturas de dados, inteligência analítica, mecanismos de governança e princípios éticos em uma arquitetura unificada para a análise de risco de fraude em CP. Do ponto de vista prático, oferece às organizações públicas uma base estruturada para o desenvolvimento de sistemas de auditoria confiáveis apoiados por IA, que promovem a transparência, a responsabilidade e a tomada de decisões baseada em evidências.

Palavras-chave: Governo Digital, Compras Públicas, Pesquisa em Ciência do Design, Dados Abertos Governamentais, Indicadores de Risco

Abstract

Public procurement (PP) accounts for a substantial share of government expenditure and remains highly vulnerable to fraud, corruption, and other irregularities. Although advances in artificial intelligence (AI) and Open Government Data (OGD) have created new opportunities for supporting oversight activities, existing studies predominantly emphasize isolated analytical techniques while overlooking the broader data, organizational, governance, and ethical conditions required for their effective adoption in public auditing. This thesis aims to design and evaluate a reference model for data-driven fraud risk analysis in PP that integrates analytical, socio-technical, governance, and ethical perspectives into a unified decision-support approach. Rather than focusing on automated fraud detection, the proposed model supports auditors in identifying, prioritizing, and investigating fraud risk indicators through transparent and accountable analytical processes. The research follows the Design Science Research paradigm, combining systematic literature reviews, expert interviews, quantitative and qualitative empirical studies, and artifact evaluation. The research includes (i) a comparative assessment of procurement OGD ecosystems in Brazil, the Netherlands, and the European Union through quantitative data quality metrics and socio-technical analysis; (ii) the construction of a catalog of fraud risk indicators supported by heterogeneous government datasets; (iii) the design of a layered Reference Model comprising Data, Engine, Decision, Ethical, Provenance, Governance and Security, and Evaluation and Refinement layers; and (iv) the development and evaluation of a prototype using Brazilian procurement data with public auditors. The results demonstrate that effective fraud risk analysis depends not only on AI models but also on the availability of interoperable and high-quality data, institutional governance, human oversight, explainability, provenance, and continuous evaluation mechanisms. The comparative analysis further shows that data quality alone does not determine analytical capability, which also emerges from legal, organizational, and cultural conditions shaping procurement data ecosystems. The proposed reference model was positively evaluated by public auditors and demonstrated its ability to support the prioritization and interpretation of fraud risk indicators while preserving human decision-making authority. This thesis contributes to Information Systems and Digital Government research by providing a sociotechnical reference model that integrates data infrastructures, analytical intelligence, governance mechanisms, and ethical principles into a unified architecture for fraud risk analysis in PP. From a practical perspective, it offers public organizations a structured foundation for developing trustworthy AI-supported auditing systems that enhance transparency, accountability, and evidence-based decision-making.

Keywords: Digital Government, Public Procurement, Design Science Research, Open Government Data, Risk Indicators

List of Figures

1.1	Government spending as a share of GDP. Extracted from Our World in Data	2
1.2	Research Design and Methodological Overview	8
2.1	Evolution of Digital Government Paradigms. Adapted from (KOWALKIEWICZ; DOOTSON, 2019)	14
2.2	Phases of the PPP.	17
2.3	Data Artifacts across the phases of PP	19
2.4	Data-Driven Decision-Making Steps	24
2.5	Key ethical principles for trustworthy AI in PP fraud detection context (Adapted from Ethics guidelines for trustworthy AI (AI, 2019))	30
2.6	Provenance Modeling Using the W3C PROV Standard. Reproduced from PROV-DM	31
2.7	Example of a PROV-Based Provenance Graph. Reproduced from PROV-DM	32
2.8	Design Science Research Cycles. Reproduced from (HEVNER, 2007) . . .	33
3.1	Information flow through the steps of the review using PRISMA Flow Di- agram - SLR I (Adapted from Moher et al (MOHER et al., 2009))	39
3.2	Information flow through the steps of the review using PRISMA Flow Di- agram - SLR II (Adapted from Moher et al (MOHER et al., 2009))	44
4.1	Research Framework. Based on (BHAROSA, 2011)	58
4.2	Reference Model	66
4.3	Data Layer	68
4.4	Engine Layer	70
4.5	Decision Layer	73
4.6	Ethical Layer	75

4.7	Our ethics-oriented pipeline for constructing trustworthy AI-based fraud detection systems for PPs. It supports the research objective of embedding ethical safeguards directly into the AI workflow, linking each stage to identified challenges.	80
4.8	E1: Lack of strategic control. This subprocess illustrates how the proposed framework addresses the absence of governance and long-term oversight in AI-based fraud detection.	81
4.9	E2: Limitations in explainability tools. This subprocess shows how the framework mitigates technical and legal shortcomings of current explainability methods.	81
4.10	E3: Lack of transparency for users. This subprocess demonstrates how the framework improves user-facing communication and understanding of AI outputs in PP.	82
4.11	E4: Lack of oversight during operation. This subprocess highlights mechanisms to ensure continuous human monitoring and intervention in AI-supported auditing.	82
4.12	E5: System opacity (black box). This subprocess illustrates how the framework reduces black-box risks by integrating explanatory layers and interactive audit dashboards.	83
4.13	Provenance Layer	84
4.14	Evaluation and Refinement Layer	86
4.15	Governance and Security Layer	88
5.1	Data Extraction and Preparation Architecture	93
5.2	Data Relationship Model of the Refined Data Layer	94
5.3	Number of Identified Red Flags per Year (2020–2024)	99
5.4	Weak Supervised Pipeline	101
5.5	Analytical Dashboard for Monitoring Procurement Risk Indicators	105
5.6	Procurement Risk Dashboard for Monitoring Contracts and Activated Red Flags	106
5.7	Case Overview and Risk Indicators	107

5.8	Activated Red Flags and Analytical Explanations	107
5.9	Supplier Information and Procurement Details	108
5.10	Data Provenance and Auditor Assessment	108
5.11	Dataset Exploration and Query Interface	109
5.12	Human in the Loop Analytical Process in the Procurement Risk Analysis Platform. Adapted from (KYRIAKOU; OTTERBACHER, 2023)	111
5.13	Provenance Representation of Data Transformations and Indicators Gen- eration in the Implemented Analytical Platform	112
5.14	RBAC Structure	114
6.1	Answers to profiling questions	120
6.2	Answers to datasets questions	122
6.3	Answers to red flags questions	123
6.4	Auditor Perceived Degree of Suspicion (Case 1)	133
6.5	Investigation Priority Assessment by Auditors (Case 1)	134
6.6	Perceived Relevance of Activated Red Flags (Case 1)	134
6.7	Auditor Agreement with Model Classification (Case 1)	135
6.8	Auditor Perceived Degree of Suspicion (Case 2)	137
6.9	Investigation Priority Assessment by Auditors (Case 2)	137
6.10	Perceived Relevance of Activated Red Flags (Case 2)	138
6.11	Auditor Agreement with Model Classification (Case 2)	139
6.12	Auditor Perceived Degree of Suspicion (Case 3)	141
6.13	Investigation Priority Assessment by Auditors (Case 3)	141
6.14	Perceived Relevance of Activated Red Flags (Case 3)	142
6.15	Auditor Agreement with Model Classification (Case 3)	143
6.16	Auditor Perceived Degree of Suspicion (Case 4)	144
6.17	Investigation Priority Assessment by Auditors (Case 4)	145
6.18	Perceived Relevance of Activated Red Flags (Case 4)	146

6.19 Auditor Agreement with Model Classification (Case 4)	146
6.20 Auditor Perceived Degree of Suspicion (Case 5)	148
6.21 Investigation Priority Assessment by Auditors (Case 5)	149
6.22 Perceived Relevance of Activated Red Flags (Case 5)	149
6.23 Auditor Agreement with Model Classification (Case 5)	150
6.24 Auditor Perceived Degree of Suspicion (Case 6)	151
6.25 Investigation Priority Assessment by Auditors (Case 6)	152
6.26 Perceived Relevance of Activated Red Flags (Case 6)	152
6.27 Auditor Agreement with Model Classification (Case 6)	153
7.1 Research Design for Analytics Capability and Data Quality Assessment . .	161
7.2 Histogram from Comparative Data Quality Assessment of Public Procurement OGD Portals	167
7.3 Integrated Comparative Assessment of Data Quality and Analytics Capability in Procurement OGD Ecosystems	175
8.1 Epistemic Cycle of Scientific Government. Inspired by (HOUGHTON, 2009)	181
8.2 Structural balance between empirical evidence, technical expertise and democratic legitimacy in public policy design	184

List of Tables

2.1	Typologies of Fraud Across the Public Procurement Cycle	21
3.1	AI Methods Categories Applied to Fraud Detection in Public Procurement	40
3.2	Classification of Data Sources in Public Procurement Fraud Detection Research	41
3.3	Fraud Types Addressed Across Reviewed Studies	41
3.4	Procurement Stages Targeted Across Reviewed Studies	42
3.5	Typology of Red Flags and Risk Indicators in Public Procurement	45
3.6	Synthesis of literature and expert interview findings and their implications for model design	53
4.1	Mapping of DSR stages to research methods and thesis chapters	60
4.2	Functional and Non-Functional Design Requirements	63
5.1	Risk Indicator Mapping to Data Sources, Calculation Procedures, and Identified Limitations	96
5.2	Distribution of Red Flag Indicators Across Procurement Contracts	98
5.3	Comparative Characteristics of Procurement Contract Clusters	101
5.4	System Interaction Logging Structure for Audit Traceability	114
6.1	Profiling Questions	121
6.2	Datasets Questions	122
6.3	Red Flags Questions	124
7.1	Data Quality Dimensions and Metrics	162
7.2	Comparative Descriptive Statistics of Datasets in Brazil, the Netherlands, and the EU	165
7.3	Comparative Data Quality Assessment of Public Procurement OGD Portals	167

7.4 Analytical Dimensions in Qualitative Assessment 170

List of Acronyms

AI	—	Artificial Intelligence
DSR	—	Design Science Research
GDP	—	Gross Domestic Product
IS	—	Information Systems
LIME	—	Local Interpretable Model-agnostic Explanations
ML	—	Machine Learning
OGD	—	Open Government Data
PNCP	—	National Public Procurement Portal
PP	—	Public Procurement
PPP	—	Public Procurement Process
SHAP	—	Shapley Additive Explanations
SLR	—	Systematic Literature Review
XAI	—	Explainable Artificial Intelligence

Thesis Publications

This section describes the papers published throughout the Ph.D. process. The first subsection presents four papers related to this work. The other subsection includes more publications during the PhD, fruits of the master's work, and partnerships with colleagues in the research group.

Related Works

- Sampaio, I., Bernardini, F., Viterbo, J., Oliveira, D., Fontes, S. (2026). Public procurement risk indicators from open government data and provenance model. International Conference on Electronic Government.
- Sampaio, I. G. B., Andrade, E. de O., Fontes, S. de S. B., Bernardini, F. C., & Viterbo, J. (2026). Trustworthy AI in public administration: The PRO-Trust pipeline for ethical fraud detection in public procurement. *Government Information Quarterly*, 43(3), 102157. <https://doi.org/10.1016/j.giq.2026.102157>
- Sampaio, I. G. B., Bernardini, F. C., & Viterbo, J. (2024, November). Challenges in Addressing the Ethical Aspects of Artificial Intelligence to Detect Fraud in Public Procurement Processes. In *Conferência Latino-Americana de Ética em Inteligência Artificial* (pp. 13-16). SBC.
- Sampaio, I., Fontes, S., Andrade, E., Bernardini, F., & Viterbo, J. (2024, June). Enhancing transparency through explainable artificial intelligence: an exploratory analysis on collusion and corruption scenario in digital government. In *Proceedings of the 25th Annual International Conference on Digital Government Research* (pp. 52-62).

Other Publications in Journals and Conferences

- Coutinho, G. B., Sampaio, I. G., Barcellos, R., & Bernardini, F. (2026, July). Viés e Discriminação no Uso de Aprendizado de Máquina em Governo Digital: Uma Re-

- visão da Literatura. In Latin American Symposium on Digital Government (LAS-DiGov) (pp. 313-324). SBC.
- Andrade, E. D. O., Guérin, J., Viterbo, J., & Sampaio, I. G. B. (2024). Adversarial attacks and defenses in person search: A systematic mapping study and taxonomy. *Image and Vision Computing*, 148, 105096.
 - Sampaio, I. G. B., Viterbo, J., & Guerin, J. (2023). Improving robustness of industrial object detection by automatic generation of synthetic images from CAD models. *Computational Intelligence*, 39(3), 415-432.
 - Andrade, E., Sampaio, I., Guérin, J., & Viterbo, J. (2023, February). Combining Two Adversarial Attacks Against Person Re-Identification Systems. In 18th International Conference on Computer Vision Theory and Applications (Vol. 5, pp. 437-444). SCITEPRESS-Science and Technology Publications.
 - Lopes, R. B., Vasconcelos, L. P., Sampaio, I. G. B., Miranda, L., Viterbo, J., & Trevisan, D. G. (2023, February). Educational Data Mining to Forecast Essay Score. A Case Study About ENEM. In International Conference on Information Technology & Systems (pp. 133-143). Cham: Springer International Publishing.
 - Sampaio, I. G. B., Andrade, E. D. O., Bernardini, F., & Viterbo, J. (2022, August). Assessing the quality of Covid-19 open data portals. In International Conference on Electronic Government (pp. 212-227). Cham: Springer International Publishing.

Contents

1	Introduction	1
1.1	Objective	6
1.2	Methodology	7
1.3	Contributions	9
1.4	Organization	10
2	Fundamental Concepts	12
2.1	Digital Government	12
2.2	Public Procurement	15
2.2.1	Procurement Data and Information Structures	17
2.2.2	Fraud in Public Procurement	19
2.3	Data, Analytics, and AI in Public Sector and Public Procurement	22
2.4	Ethical Aspects and Trustworthy AI	26
2.4.1	Defining Trustworthy AI in the Public Sector	26
2.4.2	Regulatory and Policy Frameworks for Ethical AI in Government	27
2.4.3	Core Ethical Principles for PP AI fraud detection	28
2.5	Data Provenance	30
2.6	Design Science Research	32
2.7	Final Remarks	34
3	Literature Reviews and Expert Knowledge Elicitation	36
3.1	SLR Protocol and Review Strategy	37

3.2	SLR I — Artificial Intelligence for Fraud Detection in Public Procurement	38
3.3	SLR II — Red Flags and Risk Indicators in Public Procurement	42
3.4	Synthesis of SLR Findings and Research Challenges	46
3.4.1	Strengths and Limitations of AI based Approaches	46
3.4.2	Red Flags Conceptual Robustness and Fragmentation	47
3.4.3	Structural Fragmentation and Emerging Research Challenges	48
3.5	Expert Knowledge Elicitation: Interviews with Public Auditors	49
3.5.1	Interview Context and Data Collection	49
3.5.2	Thematic Analysis of Interview Insights	50
3.5.3	Implications for Reference Model Design	52
3.5.4	Summary and Link to Artifact Requirements	53
4	Methodology, Research Design, and Artifact Development	54
4.1	Research Paradigm and Methodological Approach	54
4.2	Design Science Research Framework	56
4.2.1	DSR strategy	56
4.2.2	Mapping DSR Stages	58
4.3	Artifact Design and Development	60
4.3.1	Design Requirements	60
4.3.2	The Reference Model	63
4.3.3	Data Layer	66
4.3.4	Engine Layer	68
4.3.5	Decision Layer	72
4.3.6	Ethical Layer	74
4.3.7	Provenance Layer	83
4.3.8	Evaluation and Refinement Layer	85
4.3.9	Governance and Security Layer	87

4.4	Final Remarks	89
5	Applying the reference model	90
5.1	Data Layer	91
5.2	Engine Layer	94
5.2.1	Heuristics and Analytical Approach	94
5.2.2	AI Approach	99
5.3	Decision Layer	104
5.4	Ethical Layer	109
5.4.1	Human Oversight and Accountability	110
5.4.2	Transparency, Explainability and Provenance	111
5.5	Governance and Security Layer	113
5.6	Discussion and Limitations of the Reference Model Instantiation	115
6	Results and Evaluation	117
6.1	Evaluation Strategy	117
6.2	Expert-based Evaluation	118
6.2.1	Data sources and risk indicators	119
6.2.1.1	Qualitative insights from auditors	124
6.2.2	Case technical evaluation	131
6.2.2.1	Case 1	132
6.2.2.2	Case 2	136
6.2.2.3	Case 3	140
6.2.2.4	Case 4	144
6.2.2.5	Case 5	147
6.2.2.6	Case 6	150
6.2.3	Ethical Evaluation	154

6.3	Discussion of Results, Design Implications, and Limitations	156
7	Analytics Capability and Socio-Technical Conditions	159
7.1	Comparative Research Design	160
7.2	Quantitative Assessment of Data Quality	161
7.2.1	Quantitative Assessment: Data Quality Framework	161
7.2.2	Comparative Quantitative Results	164
7.3	Socio-technical Qualitative Analysis	169
7.3.1	Qualitative Assessment: Socio-Technical Perspectives	170
7.3.2	Comparative Qualitative Results	171
7.3.2.1	Organizational and Institutional Dimensions	171
7.3.2.2	Legal and Regulatory Dimensions	173
7.3.2.3	Cultural Dimensions	173
7.4	Final Remarks	174
8	Discussions	179
8.1	Data as the infrastructure of scientific government	179
8.1.1	Data as epistemic infrastructure and institutional awareness	180
8.1.2	Data provenance as a governance mechanism	181
8.2	Organizational and institutional implications for oversight bodies	182
8.3	Science based decision making and public policy construction	183
8.4	AI as an instrument in digital government	184
8.5	DSR as a methodological foundation for public sector innovation	185
8.6	Final Remarks	186
9	Conclusions	188
9.1	Limitations	190
9.2	Future Works	191

9.3

Final Remarks

192

References

193

Chapter 1

Introduction

Public procurement (PP) is an essential activity for the functioning of the state, enabling the acquisition of goods, services and works necessary for the implementation of public policies and the provision of services to the population (THAI, 2001). In practically all spheres of government, federal, state and municipal, the contracting processes move significant volumes of financial resources, accounting for a significant portion of the public budget (GAVUROVA; TUČEK; KOVÁČ, 2019). As illustrated in Figure 1.1, government spending as a share of Gross Domestic Product (GDP) consistently exceeds 40% in countries like Brazil, Germany and the United Kingdom, highlighting the economic magnitude of public expenditure and the need for rigorous oversight. In addition to the direct economic impact, PP exerts an influence on strategic sectors of society, such as health, education, infrastructure and security. Thus, the efficiency, transparency and integrity of these contracts are fundamental elements not only for the good use of public resources (KUMAR; NAIR; PIECHA, 2015), but also for guaranteeing rights and promoting society's trust in democratic institutions (ACHUA, 2011).

Government spending as a share of GDP, 2012 to 2022

Our World
in Data

Total government spending, including interest government expenditures, as a share of gross domestic product (GDP).

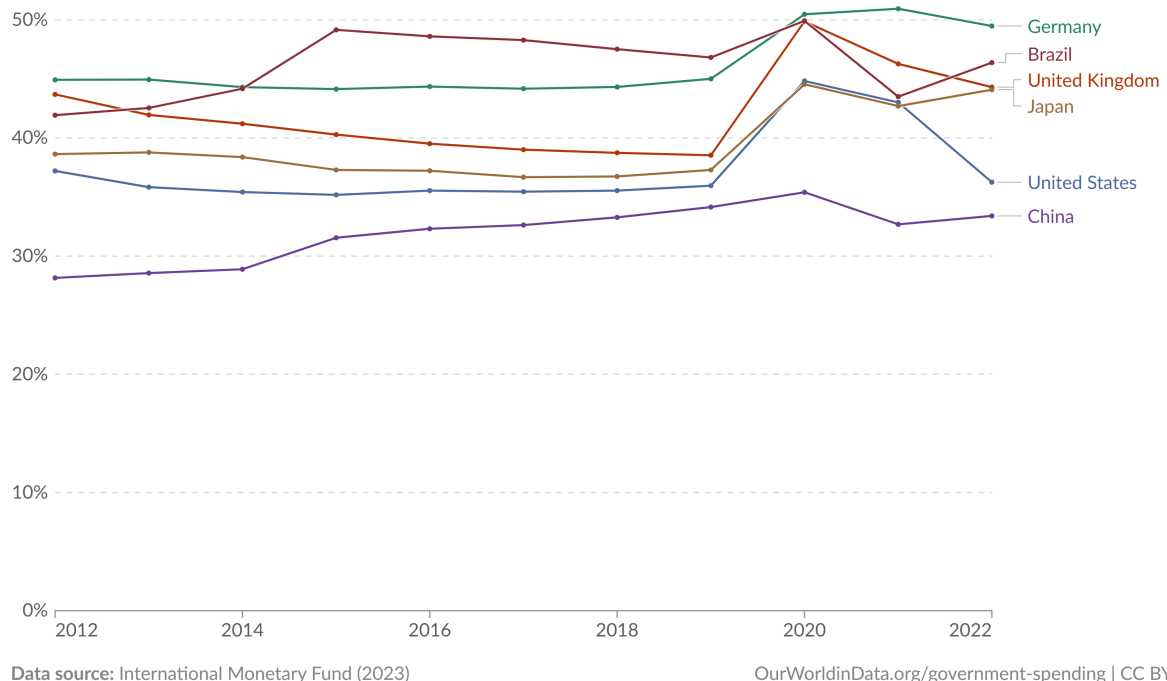


Figure 1.1: Government spending as a share of GDP. Extracted from Our World in Data

Despite their importance, PP are often the target of fraudulent practices that compromise the integrity and effectiveness of public management (RUSTIARINI; NURKHOLIS; ANDAYANI, 2019). Frauds such as overpricing, bid rigging, collusion between suppliers and improper ties between companies and public agents generate substantial financial losses for the state, diverting resources that should be applied for the benefit of society (SANTOS; SOUZA, 2016). In addition to the economic impact, these practices distort competition between market participants, discourage the participation of reputable suppliers and favor the perpetuation of corruption networks (SIROREI, 2018). Ultimately, the recurrence of fraud in PP undermines the public's trust in government institutions and weakens the pillars of democracy and social justice (ANDERSON; JONES; KOVACIC, 2024).

Historically, fraud detection in PP has been carried out through manual audits, sample analysis and investigations based on complaints or specific indications (BRANDÃO et al., 2024). Although these methods play an important role in institutional control, they have significant limitations in view of the increasing complexity and volume of data involved in contracting processes. The diversity of formats, the decentralization of systems and

the high frequency of transactions make exhaustive analysis by human teams unfeasible, which results in low preventive and reactive reach (SANTOS; SOUZA, 2016). In addition, approaches based exclusively on human expertise may be subject to cognitive biases, difficulties in standardization and delays in identifying irregularities, allowing fraudulent schemes to perpetuate themselves over time without proper confrontation.

From this perspective, fraud risk analysis can be understood as the process of identifying, assessing, and interpreting potential indicators, conditions, and patterns associated with fraudulent behavior before fraud is formally confirmed (POWER, 2013). Rather than focusing exclusively on confirmed fraud events, fraud risk analysis emphasizes the proactive evaluation of signals and vulnerabilities that may indicate elevated risks within organizational and operational processes.

In this context, the application of Artificial Intelligence (AI) techniques, especially those based on Machine Learning (ML), has proven to be a promising alternative for improving fraud detection mechanisms in PP (ALDANA; FALCÓN-CORTÉS; LARRALDE, 2022; RODRÍGUEZ et al., 2022). Unlike traditional methods, AI models are capable of analyzing large volumes of data in an automated manner, identifying complex patterns and anomalies that could go unnoticed by human analysis (NAI; SULIS; MEO, et al., 2022). By learning from historical data, these solutions can point out atypical behaviors, such as rotation of winning companies (BAROT, 2024), unusual price variations (AMIRUDDIN et al., 2024) and hidden connections between suppliers and public managers (ANDERSSON; ARBIN; ROSENQVIST, 2025). This intelligent screening capacity expands the scope and agility of control actions, allowing preventive action and more efficient allocation of audit resources.

Although the application of AI brings significant potential for improving the detection of irregularities in PP, it also raises important ethical concerns, particularly when implemented in sensitive government contexts (MURIKAH; NTHENGE; MUSYOKA, 2024). One of the main challenges lies in the lack of transparency of many AI models, especially those based on complex ML architectures often referred to as “black boxes” (ŞAHIN; ARSLAN; ÖZDEMİR, 2024). These models can produce decisions that are difficult to interpret, hindering the ability of public agents, auditors, and even affected companies to understand or contest automated outcomes. Additionally, algorithmic bias (resulting from imbalanced or unrepresentative training data) can lead to unfair classifications (MODRUŠAN; RABUZIN; MRŠIC, 2021). The absence of clear mechanisms for human oversight and accountability in AI driven processes exacerbates these issues,

undermining public trust and conflicting with the principles of legality, due process, and social control that underpin public administration.

Much of the current research and practical applications of AI in fraud detection have prioritized technical aspects such as accuracy, precision, and scalability of predictive models (BAROT, 2024; NAI; SULIS; MEO, et al., 2022). While these metrics are undoubtedly important for evaluating the performance of algorithms, this emphasis often comes at the expense of equally critical aspects, such as interpretability, explainability, and human autonomy in decision making. Many models are deployed without mechanisms that allow users, especially those in control and oversight roles to understand the rationale behind predictions or recommendations (HICKOK, 2024). In contexts like PP, where decisions can directly affect the reputation and rights of individuals and organizations, the inability to trace or justify algorithmic outputs is a significant limitation. Moreover, by disregarding the need for human in the loop approaches, many systems risk automating complex judgments without sufficient context or oversight, thereby amplifying the risks of error, bias, and injustice in public governance.

PP exhibit considerable variation across countries, shaped by distinct legal frameworks, administrative structures, and levels of digital maturity (CONCHA et al., 2012). This heterogeneity poses a significant challenge to the development of universally applicable fraud detection systems, as technical solutions must account for contextual specificities in data availability, institutional capacity, and regulatory environments. While certain nations operate under centralized and highly digitized procurement platforms, others maintain fragmented systems with varying degrees of transparency and standardization. A common trend, however, is the progressive dissemination of Open Government Data (OGD), which creates new opportunities for the application of AI in public oversight (SUSAR; AQUARO, 2019). In this regard, Brazil stands out as a country that, despite its decentralized and complex procurement ecosystem, has advanced considerably in transparency initiatives, offering a rich set of public data through platforms such as the Transparency Portal ¹, the National Public Procurement Portal (PNCP) ², among others. These conditions make the Brazilian case particularly relevant for exploring the potentials and limitations of AI based approaches in fraud detection within PP. In addition to these equally critical aspects, provenance is essential for tracing the origin and transformations of data and analytical outputs throughout the analysis process (SIMMHAN; PLALE; GANNON, et al., 2005). In fraud risk analysis, it enables auditors to trace

¹<https://portaldatransparencia.gov.br/>

²<https://www.gov.br/pncp/pt-br>

risk signals back to the analytical procedures and underlying data from which they were derived, supporting inspection, reproducibility, and auditability (SAMPAIO; BERNARDINI; VITERBO, et al., 2026).

In the context of PP fraud detection, risk indicators commonly referred to as red flags play a crucial role in identifying atypical patterns and guiding investigative efforts (BAROT, 2024). These indicators are based on characteristics or behaviors that deviate from expected norms and may signal irregularities, such as repeated awards to the same supplier (HORNE; VENTER; LOCHNER, 2018), unusually short bidding periods (MODRUŠAN; RABUZIN; MRŠIC, 2021), or price deviations in similar contracts (TÁTRAI; NÉMETH, 2018). Unlike opaque algorithmic outputs, red flags are generally constructed to be interpretable, offering a bridge between automated analysis and human judgment. They allow auditors, analysts, and oversight bodies to prioritize cases for deeper investigation, facilitating a more efficient allocation of resources. Moreover, red flags can be derived from domain knowledge and empirical evidence, making them adaptable to specific legal, institutional, and cultural contexts (MILANI, 2019). When integrated with AI models, they can enhance transparency, foster explainability, and increase the overall trustworthiness of fraud detection systems in the public sector.

Given the risks associated with opaque and overly technical AI applications in sensitive government contexts, it becomes imperative to promote an integrated approach that combines analytical performance —+*— with ethical and institutional adequacy. Fraud detection systems must not only be capable of identifying suspicious patterns but also provide mechanisms that support transparency, accountability, and informed human oversight. However, much of the existing research addresses isolated aspects of this problem, focusing either on specific analytical techniques, individual risk indicators, or particular datasets, without offering a comprehensive perspective on how these elements can be systematically integrated into a coherent analytical framework. In practice, effective fraud risk analysis in PP requires a broader perspective that connects data sources, analytical procedures, and decision support mechanisms while remaining adaptable to different institutional and technological contexts. A reference model provides such a structure by defining the essential concepts, components, and relationships of a domain at an abstract level, serving as a reusable basis for the development of context-specific solutions (BECKER; DELFMANN; KNACKSTEDT, 2007) rather than prescribing a single implementation. This includes the transformation of heterogeneous data sources, such as OGD, into structured risk indicators, the application of analytical methods capable of generating actionable intelligence, and the integration of these outputs into decision support

environments that assist auditors and oversight bodies in their investigative processes. Furthermore, such architectures must incorporate ethical and governance considerations as cross cutting elements that permeate the entire analytical pipeline. It is precisely this structural gap, between the availability of data, the generation of analytical insights, and their effective use in decision support systems for public oversight, that this research seeks to address.

1.1 Objective

The main objective of this thesis is to design, implement, and evaluate a reference model for fraud risk analysis in PP. The proposed reference model comprises a core analytical framework structured around data integration, analytical modeling, and decision support layers combined with institutional components addressing ethical principles, governance and security, and iterative evaluation and refinement. Rather than emphasizing predictive accuracy alone, the model integrates domain informed red flags, explainable ML, and end to end traceability mechanisms to ensure transparency, auditability, and human oversight. By grounding the artifact in real procurement processes, structuring risk signals that reflect actual auditing practice, and embedding mechanisms that make analytical outputs intelligible to oversight professionals, this thesis advances both the technical foundations and the institutional legitimacy of AI assisted fraud risk analysis.

To achieve this objective, the research undertakes a sequence of interconnected stages: (i) conducting two systematic literature reviews, one focused on AI based approaches to fraud detection and another on red flag based risk indicators in PP, in order to identify technical, methodological, and governance-related gaps in the existing literature. Complementing the insights derived from the literature, a series of semi-structured interviews was conducted with Brazilian public auditors in order to capture practical perspectives on fraud detection processes, commonly used analytical practices, and the operational relevance of different risk indicators. These interviews provided empirical grounding for the design of the proposed framework and helped align the analytical components of the model with real auditing practices. Building on these theoretical and empirical inputs, the research then proceeds with (ii) the design of a reference model that integrates a core analytical layer comprising data, engine, and decision layers with institutional components addressing ethical principles, governance and security, and iterative evaluation and refinement; (iii) the instantiation of the proposed reference model in real world procurement contexts through the operationalization of its analytical and decision support components

using OGD; and (iv) the evaluation of the reference model through qualitative analysis and structured interaction with public auditors, including a comparative assessment between Brazil, European Union and the Netherlands to examine its analytical capability, institutional alignment, and adaptability across distinct governance environments.

1.2 Methodology

This research adopts a Design Science Research (DSR) approach to develop, instantiate, and evaluate the reference model for fraud risk analysis in public procurement. Consistent with DSR guidelines, the methodological design integrates qualitative and quantitative techniques across iterative build and evaluate cycles, ensuring that the artifact is simultaneously grounded in domain knowledge, informed by scientific rigor, and aligned with the practical needs of oversight institutions. The research process unfolds across interconnected phases that progressively transform OGD into interpretable risk signals, ML models, and explainable outputs validated with domain experts.

The first phase establishes the theoretical and empirical foundations of the study. It comprises two systematic literature reviews: one examining AI based approaches to fraud detection and another focusing on red flag based risk indicators in public procurement. These reviews identify technical, methodological, and governance related gaps in the literature, particularly concerning transparency, interpretability, and institutional alignment of AI based fraud detection systems. Complementing the insights derived from the literature, a series of semi structured interviews was conducted with Brazilian public auditors in order to capture domain specific practices, investigative procedures, and operational constraints associated with fraud detection in procurement processes. The interviews also contributed to identifying relevant risk indicators, data usage practices, and expectations regarding analytical tools that could support oversight activities. Together, the literature reviews and expert interviews define the problem space, clarify institutional requirements, and provide the empirical grounding that guides the subsequent design of the proposed artifact.

Building upon the identified foundations and requirements, the second phase focuses on the design of the proposed reference model. This model integrates a core analytical framework comprising data, engine, and decision layers with complementary components addressing ethical principles, governance and security, and iterative evaluation and refinement.

The third phase involves the instantiation and evaluation of the Reference Model in real procurement contexts. The artifact is assessed through structured interaction with public auditors, examining its analytical utility, interpretability, and institutional adequacy. Empirical instantiation enables the examination of how the model operates in practice, while a comparative analysis between Brazil, European Union and the Netherlands explores how differences in governance, legal frameworks, and data ecosystems influence its applicability and responsible deployment. This phase ensures that the proposed model is not only theoretically coherent but also practically relevant and contextually adaptable.

The overall methodological structure of the research linking the PP context and research problem to the foundations and requirements stage, the development of the reference model, and its subsequent evaluation is summarized in Figure 1.2.

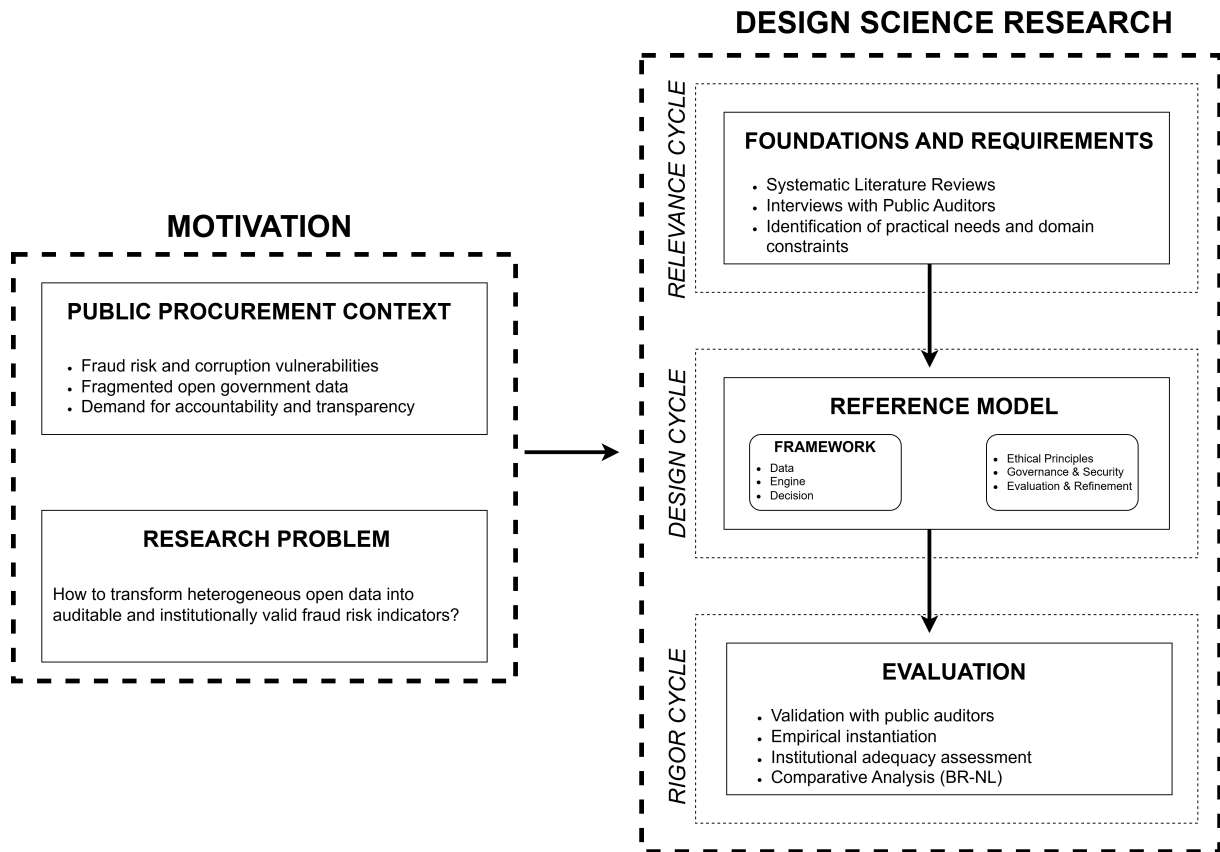


Figure 1.2: Research Design and Methodological Overview

1.3 Contributions

This thesis makes theoretical, methodological, and practical contributions to the fields of digital government, data science, and PP oversight by developing and evaluating a reference model for fraud risk analysis grounded in OGD. Rather than focusing on predictive performance, the research advances a structured and governance oriented perspective on AI assisted oversight, emphasizing interpretability, traceability, institutional alignment, and responsible deployment in high stakes public sector environments.

From a theoretical perspective, the thesis contributes by conceptualizing fraud risk analysis in PP as a sociotechnical design problem and by formalizing a reference model that integrates a core analytical framework (data, engine, and decision layers) with complementary governance components addressing ethical principles, security, and iterative refinement. By combining AI based analytical mechanisms with structured red flag logic and institutional constraints, the research clarifies how heterogeneous OGD can be transformed into auditable and institutionally grounded fraud risk indicators.

Methodologically, this thesis contributes by demonstrating how DSR can be effectively applied to complex challenges in digital government, particularly in the domain of PP oversight. Rather than treating fraud detection as a purely technical or predictive task, the research frames it as a sociotechnical design problem that requires the integration of scientific artifacts, including DSR principles, data science techniques, and systematic research methods within institutional decision making environments. By combining structured literature synthesis, analytical modeling, and empirical engagement with Brazilian public auditors, the study illustrates how scientific methodologies can be operationalized to address real world governmental problems. In doing so, it advances the methodological understanding of how research driven artifacts can move beyond experimental settings and be embedded within public sector workflows, balancing analytical innovation with institutional legitimacy and practitioner knowledge.

From a practical standpoint, the research delivers a reference model that supports fraud risk analysis in PP through structured red flags, interpretable analytical flows, and governance oriented design principles. By formalizing how risk indicators are constructed, operationalized, and assessed within institutional constraints, the model provides oversight bodies with a transparent and adaptable foundation for decision support. The comparative analysis between Brazil, European Union and the Netherlands further extends the contribution by examining how variations in legal, administrative, and data governance

environments influence the applicability and ethical implications of AI assisted oversight, offering insights into the transferability of the model across jurisdictions.

Collectively, these contributions position the thesis at the intersection of digital government, public administration, and data science, offering a reference model for trustworthy and institutionally aligned fraud risk analysis in PP.

1.4 Organization

This thesis is organized into nine chapters, structured to reflect the progressive development, instantiation, and evaluation of the proposed reference model for fraud risk analysis in PP. Chapter 2 presents the fundamental concepts that underpin the research. It introduces the evolution of digital government, public procurement and its fraud-related challenges, the role of data, analytics, and artificial intelligence in the public sector, ethical principles for trustworthy AI, and data provenance as a mechanism for transparency, traceability, and accountability. The chapter concludes with an overview of the Design Science Research paradigm, which provides the methodological foundation for the development of the proposed reference model.

Chapter 3 reports the knowledge acquisition activities that inform the design of the proposed reference model. It presents two systematic literature reviews, one on AI-based fraud detection in public procurement and another on red flag-based risk indicators, followed by expert interviews with Brazilian public auditors. Together, these activities establish the theoretical foundations, identify practical requirements, and provide the institutional insights that underpin the development of the proposed reference model.

Chapter 4 details the methodological design and artifact development process. Grounded in Design Science Research, it presents the research design, derives the artifact design requirements, and introduces the proposed reference model, integrating a core analytical framework (data, engine, and decision layers) with complementary components addressing ethical principles, governance and security, provenance, and iterative evaluation and refinement.

Chapter 5 presents the instantiation of the proposed reference model in the Brazilian public procurement context. It describes the implementation of the model's layers, including data integration, risk indicator generation, AI-supported analytics, decision support functionalities, and mechanisms for transparency, provenance, governance, and security, demonstrating how the reference model can be operationalized in practice.

Chapter 6 presents the evaluation of the proposed reference model through empirical studies involving public auditors. It reports the results of expert-based assessments of the data sources, risk indicators, analytical outputs, and ethical aspects of the model, examining its practical applicability, interpretability, and institutional adequacy.

Chapter 7 presents a comparative assessment of procurement OGD ecosystems in Brazil, the Netherlands, and the European Union. It combines a quantitative evaluation of data quality with a qualitative socio-technical analysis of the organizational, institutional, legal, and cultural conditions that shape analytics capability for PP oversight.

Chapter 8 discusses the broader implications of the research for digital government and public sector innovation. It reflects on the role of data, analytics, and AI in supporting evidence-based oversight while examining the organizational, governance, methodological, and societal implications of the proposed reference model.

Chapter 9 concludes the thesis by summarizing its main theoretical, methodological, and practical contributions, emphasizing the proposed reference model for data-driven fraud risk analysis in public procurement. It also discusses the study's limitations and outlines directions for future research and the practical adoption of trustworthy AI-enabled decision support in public procurement oversight.

Chapter 2

Fundamental Concepts

This chapter presents the fundamental concepts that underpin the development of the thesis. It begins by examining the evolution of digital government and the role of public procurement within contemporary public administration, introducing its organizational characteristics, information structures, and fraud-related challenges. Building on this foundation, the chapter discusses the growing role of data, analytics, and artificial intelligence in supporting public sector decision-making and oversight, followed by an examination of the ethical principles and regulatory perspectives that underpin trustworthy AI. It then introduces data provenance as a mechanism for enhancing transparency, traceability, and accountability in analytical ecosystems. Finally, the chapter presents the Design Science Research paradigm, which provides the methodological foundation for the design, instantiation, and evaluation of the proposed reference model.

2.1 Digital Government

Digital government has emerged as a foundational paradigm for modern public administration, reflecting the increasing centrality of digital technologies, data infrastructures, and information governance in state operations (SETYAWAN, 2024). International organizations provide complementary definitions that collectively shape the conceptual landscape of the field (AMORETTI, 2007). Panagiotopoulos et al. (PANAGIOTOPOULOS; KLIEVINK; CORDELLA, 2019) frames digital government as the strategic use of digital technologies to foster openness, citizen engagement, and public value creation, emphasizing governance models in which data and platforms are key enablers of policy and service innovation. A different strand of the literature conceptualizes digital government as a sociotechnical transformation of the state, in which organizational structures, adminis-

trative processes, and public sector capabilities are redesigned to operate effectively in a data intensive, networked environment (GIBREEL; HONG, 2017). This perspective underscores the shift from siloed, paper based bureaucracies to integrated, process oriented and analytics enabled administrations, where digital technologies support coordination, evidence driven decision-making, and proactive service delivery. Together, these definitions converge on the idea that digital government represents not merely the digitization of public services, but a systemic transformation in which data, platforms, and interoperable infrastructures become foundational elements of contemporary governance.

The evolution of digital government can be understood as a progression of interconnected phases. Early digital government initiatives focused primarily on providing online access to information and services, mirroring administrative processes in digital form (FANG, 2002). As technologies matured, governments adopted more integrated architectures, giving rise to digital government, characterized by service interoperability (CAMPMAS; IACOB; SIMONELLI, 2022), platform based delivery models (NAM; NAM; KIM, 2024), and process automation (LINDGREN, 2020). The subsequent emergence of data driven government shifted the emphasis toward analytics and the systemic use of administrative data as a strategic asset for planning, monitoring, and policy formulation (ANSHARI; LIM, 2017). More recently, advancements in AI, ML, and automated decision systems have introduced the notion of algorithmic government, in which computational models increasingly support or shape administrative decisions and oversight activities (ENGIN; TRELEAVEN, 2019).

This historical trajectory reflects a broader conceptual shift: from digitizing isolated services to coordinating systems, and ultimately to decisions through data. Contemporary digital government frameworks place strong emphasis on enabling infrastructures such as interoperable registries, secure data exchange mechanisms, and common platforms that allow information to flow across organizational boundaries. This shift advances not only administrative efficiency but also new forms of transparency, accountability, and value with citizens and stakeholders.

Across its evolution, digital government has undergone a structural transformation that extends beyond technological modernization to encompass shifts in service logic, organizational models, and performance priorities. As illustrated in Figure 2.1, this trajectory unfolds across five stages. Digital Government 1.0 (Emergence) centers on individual service delivery, prioritizing service access and quality. In Digital Government 2.0 (Industrialising), the focus shifts toward scaling service provision, emphasizing value chain

coordination and equitability. The Automation phase (3.0) advances efficiency through operating model optimization and practicality driven performance. With Digitalisation (4.0), the emphasis moves toward whole-of-government integration, business model transformation, and connectivity across departments. Finally, Personalisation (5.0) reflects a citizen-centered model oriented toward whole-of-life service delivery, desirability, and cross-government collaboration. Across these stages, digital government progressively transitions from isolated service provision to integrated, citizen-driven ecosystems supported by increasingly coordinated institutional arrangements and data infrastructures. This evolution creates the structural conditions for advanced analytical oversight mechanisms by increasing data availability, institutional interconnectivity, and the demand for transparent, accountable, and explainable decision support systems.

Evolution	1.0	2.0	3.0	4.0	5.0
Title	EMERGENCE	INDUSTRIALISING	AUTOMATION	DIGITALISATION	PERSONALISATION
Description	Individual service delivery	Scaling service delivery (volume/variety)	Efficient service delivery	Whole-of-government service delivery	Whole-of-Life service delivery
Focus	Service access	Value chain	Operating model	Business model	Citizen model
KPI	Quality	Equitability	Practicality	Connectivity	Desireability
Enablers	Service designers	Operating officers (volume) Service designers (variety)	Operating officers	Cross-department teams Whole-of-government experience designers	Cross-government teams and partnerships

Figure 2.1: Evolution of Digital Government Paradigms. Adapted from (KOWALKIEWICZ; DOOTSON, 2019)

The consolidation of digital government thus establishes the institutional and technological foundations upon which more specialized administrative domains operate (LUNA-REYES; GIL-GARCIA, 2014). As public administrations adopt platform based architectures, interoperable systems, and data frameworks, they create environments capable of generating structured, high quality information that can support increasingly sophisticated forms of oversight, evaluation, and decision making. These developments have broadened the analytical capacity of governments and, at the same time, heightened expectations regarding transparency, traceability, and evidence based public management

(SHARMIN; CHOWDHURY, 2025).

Within this broader transformation, specific policy areas have become particularly dependent on digital infrastructures and data-driven practices. PP is one of the most prominent examples, both because of its scale and because of the volume and granularity of information it produces throughout the contracting cycle (FELIZZOLA et al., 2024). The increasing digitalization of procurement processes not only reflects the principles discussed in this section but also exemplifies how digital government initiatives enable new forms of monitoring, accountability, and risk analysis. These developments are particularly consequential in domains where administrative processes generate extensive digital traces, such as PP. Exploring this domain in greater depth helps illuminate how digital infrastructures shape operational complexity, transparency demands, and opportunities for enhanced oversight.

2.2 Public Procurement

PP refers to the set of processes by which governments acquire goods, services, and public works necessary for fulfilling their functions (BERMÚDEZ; FARIAS; TORRES, 2020). It is recognized by international organizations such as the OECD, the World Bank, and the European Commission as one of the most significant economic and administrative activities of the state, up to 25% of national GDP (FAZEKAS; BLUM, 2021). Beyond its fiscal magnitude, procurement serves as a strategic policy instrument: it supports the delivery of essential public services, stimulates economic development, fosters innovation, and promotes social outcomes through regulatory mechanisms such as sustainable or inclusive purchasing (KULLMANN, 2018). Fundamentally, procurement systems are guided by principles of legality, fairness, competition, efficiency, transparency, and accountability (HERMAN; YOHANNIS, 2018). These principles aim to ensure that public resources are used effectively and that contracting decisions are made in accordance with established norms. As a result, procurement is not merely a transactional function but a governance mechanism that shapes how public value is created and distributed across society.

The procurement processes is shaped by a wide array of actors whose roles and interactions influence both procedural integrity and administrative outcomes. Contracting authorities and procuring units oversee the planning, preparation, and execution of procurement procedures, while economic operators participate competitively under legally established frameworks. A second layer of institutional actors—including internal con-

trol bodies, legal advisors, and procurement committees—supports procedural compliance and ensures adherence to regulatory standards. External oversight institutions, such as supreme audit bodies and anti-corruption agencies, further contribute to accountability by monitoring outcomes and investigating irregularities.

These actors operate within governance arrangements defined by statutory requirements, institutional mandates, and administrative traditions (THAI, 2017). In many jurisdictions, centralized procurement authorities are responsible for issuing regulatory guidelines, administering e-procurement infrastructures, and promoting the standardization of procedures across public organizations (MCCUE; PITZER, 2000). Sectoral agencies and subnational entities, in turn, adapt these directives to their operational contexts, taking into account organizational capacities, budgetary constraints, and domain specific requirements (SCHMITZ et al., 2025). This multilayered governance structure, characteristic of contemporary procurement systems, creates opportunities for coordination, interoperability, and professionalization. At the same time, it introduces challenges arising from institutional fragmentation, heterogeneous levels of digital maturity, and inconsistencies in the implementation of integrity and compliance safeguards (MANTA; MANSI, 2024).

Figure 2.2 illustrates the main public procurement process as defined in Article 17 of Brazilian Law No. 14.133/2021¹. Although procurement procedures vary across jurisdictions due to differences in legal frameworks and administrative traditions, the Brazilian model is used here as a guiding reference to structure the discussion. The process typically begins with the Preparatory Phase, which involves internal planning, needs assessment, and the drafting of technical specifications. This is followed by the Tender Notice Publication, formally initiating the competitive procedure. Suppliers then proceed with the Submission of Proposals, after which bids are examined during the Bid Evaluation Phase, where they are assessed according to predefined criteria. The Qualification Verification Phase ensures that the selected bidder meets legal, fiscal, and technical requirements. Subsequently, the Appeals Phase allows participants to challenge procedural or evaluation decisions. The process concludes with the Formal Approval (Ratification) Phase and the Contract Award Phase, which validate the procedure and formally assign the contract to the winning bidder. While procedural sequences and terminology may differ across countries, these stages represent common structural elements of competitive public procurement systems.

¹https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm

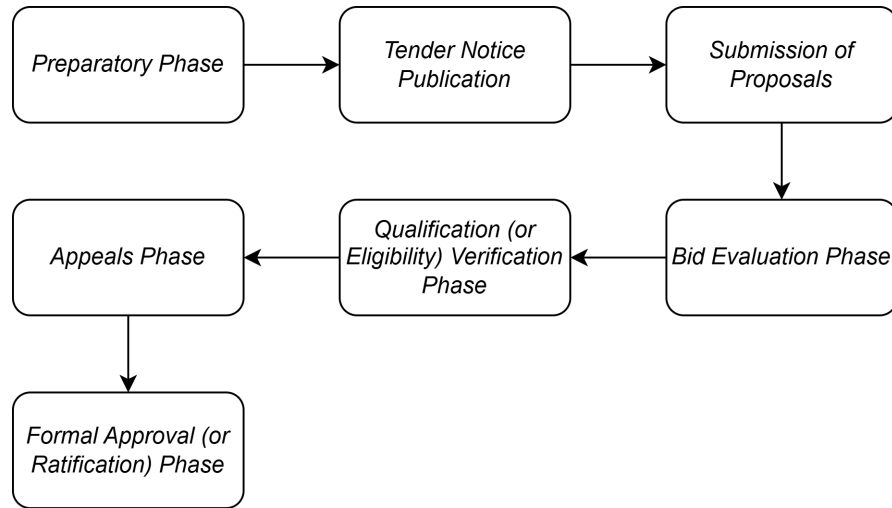


Figure 2.2: Phases of the PPP.

2.2.1 Procurement Data and Information Structures

The digital transformation of PP has fundamentally reshaped how contracting processes are conducted, documented, and monitored. E-procurement platforms consolidate procedures that were previously dispersed across agencies and formats, providing standardized workflows, integrated registries, and structured digital records (REBUGLIO; OTTAVIANI; DE MARCO, 2025). These systems enable governments to automate procedural steps, reduce administrative burden, and increase the efficiency and transparency of procurement activities (LUNGU, 2024). By centralizing information flows, digital platforms also strengthen compliance mechanisms, facilitate real time publication of procurement data, and support the adoption of advanced analytical tools.

In the Brazilian case, the digital ecosystem is anchored in platforms such as Compras-Net² and the National Public Procurement Portal (PNCP)³, which aggregate federal, state, and municipal procurement information and promote standardization through unified procedures and data structures (LABORATÓRIO DE INOVAÇÃO EM GOVERNO et al., 2021). Although these systems represent significant progress, the coexistence of legacy databases, heterogeneous adherence to national standards, and disparities in digital maturity across subnational entities contribute to fragmentation and inconsistent data quality (OLIVEIRA, 2024). Furthermore, since the enactment of Law No. 14.133/2021, contracting authorities have been permitted to operate independent electronic procurement portals, provided that procurement data are integrated with the PNCP. While this

²<https://www.gov.br/compras/pt-br>

³<https://www.gov.br/pncp/pt-br>

measure expands flexibility and autonomy at the subnational level, it also introduces additional layers of technical heterogeneity, synchronization challenges, and data integration inconsistencies, thereby complicating efforts to ensure completeness, interoperability, and uniform data governance. Integration with budgetary, financial, and contract management systems remains uneven, further constraining the construction of a fully interoperable procurement information infrastructure.

PP is an inherently data intensive domain, generating a wide range of informational artifacts across its lifecycle including planning documents, tender notices, supplier submissions, evaluation records, contract metadata, invoices, inspections, amendments, and audit reports which collectively create a rich environment for transparency, monitoring, and risk analysis (FELIZZOLA et al., 2024). The heterogeneity, granularity, and volume of these datasets make procurement particularly suitable for data driven oversight, yet also expose critical limitations: missing fields, inconsistent identifiers, unstructured attachments, and incomplete metadata hinder interoperability and obstruct the reconstruction of end to end procurement histories (DUGUAY; RAUTER; SAMUELS, 2023). Moreover, the use of divergent coding standards and taxonomies across IS reduces comparability and undermines the integration of datasets from multiple sources.

Figure 2.3 presents the main categories of data generated across the PP lifecycle, structured according to the phases previously described: Preparatory Phase, Tender Notice Publication, Submission of Proposals, Bid Evaluation Phase, followed by the post award stages of Contract Execution and Oversight and Payment. For each phase, the figure illustrates the corresponding data artifacts produced, highlighting the progressive accumulation of information throughout the process. In the preparatory stage, documents such as price quotations, budget estimates, and procurement plans are generated. The publication stage produces tender notices, technical specifications, evaluation criteria, and legal requirements. During proposal submission, bidding auction data and supplier documentation are recorded, while the bid evaluation phase results in formal bidding outcomes. The post procurement stages (visually distinguished in orange) capture contract execution artifacts, including contract documents and orders, as well as oversight and payment records such as invoices. In the figure, white document icons represent predominantly unstructured data, typically composed of textual or document based information, whereas gray document icons indicate structured data, generally stored in tabular or transactional systems. This distinction reflects the transition from document heavy, semi-structured information in earlier stages to more standardized and database oriented records in later phases. It is important to note that not all artifacts represented are fully accessible to

the public, as legal and institutional restrictions may apply. Moreover, the figure reflects a canonical procurement workflow and does not explicitly incorporate exceptional procedures or alternative contracting modalities. Overall, the diversity and heterogeneity of these data structures illustrate both the analytical potential and the operational challenges associated with transparency, monitoring, and fraud risk analysis in public procurement systems.

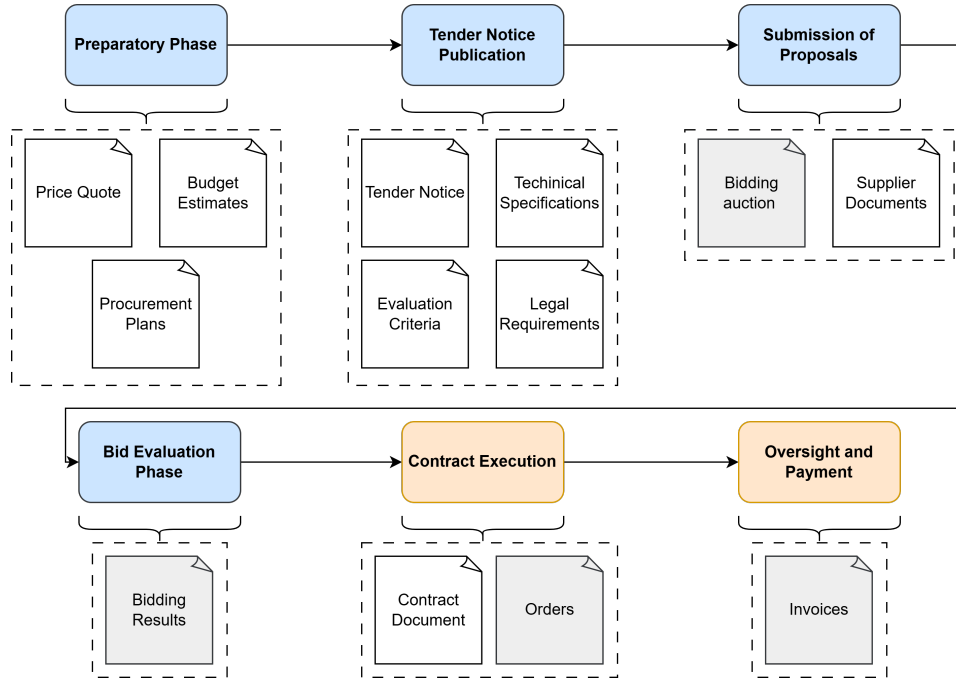


Figure 2.3: Data Artifacts across the phases of PP

2.2.2 Fraud in Public Procurement

Fraud in PP refers to the intentional manipulation of contracting processes with the purpose of securing an unlawful benefit or causing financial or operational harm to the public administration (WEINGÄRTNER et al., 2021). It is distinguished by deliberate intent and concealment, setting it apart from inadvertent procedural errors or administrative irregularities. The literature often situates procurement fraud within a broader family of illicit practices, including corruption, typically involving the abuse of public authority for private gain, and collusion, where bidders coordinate to distort competitive outcomes (NAI; SULIS; MEO, et al., 2022; RUSTIARINI; NURKHOLIS; ANDAYANI, 2019; RENDON; RENDON, 2015). While these practices may overlap in complex cases, fraud in procurement specifically denotes intentional misconduct that undermines the principles of competition, transparency, and fairness that structure public contracting systems (ALVES BATISTA, 2024). This conceptual foundation provides a basis for examining the mech-

anisms, risk factors, and detectable signals that characterize fraudulent behaviors in the procurement lifecycle.

Conceptually, fraud can be understood as a violation of process integrity throughout the procurement cycle (HEGGSTAD; FRØYSTAD, 2011). This perspective highlights that fraudulent schemes may emerge at any stage, from needs assessment and tender preparation to supplier selection, contract execution, and payment and often exploit asymmetries of information, gaps in oversight, or systemic vulnerabilities. Fraud is thus embedded within broader institutional and regulatory contexts: the design of procurement laws, the maturity of digital systems, the capacity of oversight bodies, and the culture of integrity within public organizations all influence both the opportunities for fraudulent behavior and the mechanisms through which it can be detected or concealed. The multidimensional nature of fraud underscores the need for analytical frameworks capable of integrating procedural, behavioral, and data-driven perspectives (ALTURKI et al., 2020). Traditional auditing methods rely on ex post inspection and documentary verification, but digital procurement environments generate new possibilities and challenges for identifying suspicious patterns (SANTOS; SOUZA, 2016).

Fraud in PP manifests in diverse forms that correspond to the structural and procedural characteristics of each phase of the contracting cycle. Because procurement consists of sequential stages: planning, tender preparation, bidding, evaluation, contracting, and execution, fraudulent schemes often exploit vulnerabilities specific to each step (MODRUŠAN; RABUZIN; MRŠIC, 2021). A process oriented typology therefore allows for a more precise understanding of how irregularities emerge, how they are coordinated, and which institutional controls they attempt to circumvent.

Pre-tendering fraud generally involves manipulating the definition of needs, technical specifications, or cost estimates to favor a particular supplier or to artificially justify procurement decisions (MANTZARIS, 2014). Examples include tailoring specifications to a preselected vendor, fragmenting contracts to avoid competitive procedures, inflating estimated prices, or restricting market research to a narrow group of potential bidders.

Tendering phase fraud often consists of practices that undermine competition during the bidding process. Common schemes include bid suppression, complementary bids, rotation of winners, and other forms of collusive behavior among suppliers (WEISHAAR, 2013). Procedural manipulation such as controlling access to tender documentation, restricting deadlines, or leaking confidential information also appears at this stage and can significantly distort competitive dynamics.

Evaluation and award fraud occurs when the assessment of proposals is intentionally biased or formally manipulated. This may involve arbitrary disqualification of competing offers, unjustified scoring adjustments, preferential interpretation of criteria, or the selection of a higher priced bidder without legitimate justification (ALVES BATISTA, 2024). Such actions typically rely on exploiting discretionary elements of evaluation procedures.

Contract execution fraud comprises irregularities that arise after the contract has been awarded. These include systematic overbilling, delivery of substandard or incomplete goods and services, unauthorized subcontracting, false invoicing, and misuse of contractual amendments to increase prices or extend deadlines without valid cause (ABIORO, 2021). Execution related fraud is particularly difficult to detect because it often depends on informational asymmetries between contracting authorities and suppliers, and because documentation may be incomplete or inconsistently recorded.

Table 2.1 synthesizes the principal categories of fraud observed across the PP cycle. The table organizes fraudulent schemes according to the procedural stage in which they typically occur, highlighting how vulnerabilities differ between planning, tendering, bidding, evaluation, contract execution, and oversight. This structured typology supports a process oriented understanding of procurement fraud and serves as a foundation for the discussion of red flags and detection mechanisms in subsequent sections.

Table 2.1: Typologies of Fraud Across the Public Procurement Cycle

Phase	Fraud Type	Reference
Pre-Tendering	Manipulation of needs assessments; tailoring of technical specifications; inflated cost estimates; contract splitting to avoid competitive procedures; restricted market research.	(MODRUŠAN; RABUZIN; MRŠIC, 2021)
Tender Preparation and Publication	Design of tender documents favoring a specific supplier; restrictive or discriminatory requirements; limited access to tender information; manipulation of deadlines.	(GRAYCAR, 2019)
Bidding Phase	Bid rigging and collusion; rotation of winning bidders; suppression of competition; artificial bid submissions; leakage of confidential information.	(RODRÍGUEZ et al., 2022)
Evaluation and Award	Unjustified disqualification of bidders; biased scoring; manipulation of evaluation criteria; awarding contracts at inflated prices without justification.	(MANTZARIS, 2014)
Contract Execution	Delivery of substandard or incomplete goods or services; overbilling and false invoicing; unauthorized subcontracting; irregular amendments increasing price or scope.	(MATTHEW; PATRICK; DENISE, 2013)
Oversight and Payment	Manipulated inspection or performance reports; approval of payments without verification; alteration or destruction of records to conceal irregularities.	(RENDON; RENDON, 2015)

Supreme audit institutions, internal control bodies, and anti-corruption agencies employ a variety of mechanisms to detect irregularities in PP, with red flags playing a central

role as indicators of elevated fraud or corruption risk. In Brazil, institutions such as the Tribunal de Contas da União (TCU) and the Controladoria Geral da União (CGU) incorporate risk indicators into their audit methodologies to prioritize contracts, identify anomalous patterns, and support investigative procedures. International organizations, including SIGMA/OECD, INTOSAI, and the Open Contracting Partnership (OCP), have likewise developed extensive red flag catalogues to guide oversight practices worldwide. Red flags may be quantitative, such as unusually high prices, limited competition, excessive amendments, or atypical bidding behavior or qualitative, capturing procedural inconsistencies, conflicts of interest, or governance weaknesses. Importantly, these indicators function as heuristics rather than definitive proof of wrongdoing; their strength lies in their interpretability, transparency, and alignment with domain expertise, making them foundational both to traditional auditing and to contemporary data-driven oversight approaches.

Despite the availability of such mechanisms, fraud detection in public procurement remains complex and resource intensive. Fragmented information infrastructures, heterogeneous data structures, inconsistent identifiers, and uneven digital maturity hinder the reconstruction of procurement histories and constrain large scale analytical monitoring. Data quality issues, including incomplete records, missing metadata, and unstructured attachments, further complicate automated analysis. These challenges are exacerbated by the scarcity of confirmed fraud labels, which limits the applicability of supervised learning techniques and increases reliance on heuristic, anomaly based, or hybrid detection strategies. Institutional and legal frameworks also shape detection capacities: in Brazil, Law No. 14.133/2021 emphasizes transparency, digital integration, and risk management, complemented by TCU and CGU oversight mechanisms; within the European Union, harmonized procurement directives and oversight bodies such as the European Court of Auditors promote standardization and accountability across Member States. Although implementation varies, fraud risk in public procurement emerges within structured yet imperfect regulatory environments.

2.3 Data, Analytics, and AI in Public Sector and Public Procurement

The growing digitalization of governmental activities and the expansion of OGD initiatives have significantly increased the volume, diversity, and availability of public sector data (CHARALABIDIS et al., 2018). In parallel, advances in information systems, data

infrastructures, and analytical capabilities have progressively transformed how public organizations support planning, monitoring, and operational activities (NWAIMO; OLU-OHA; OYEDOKUN, 2019). Within this context, the concept of Data-Driven Decision-Making (DDDM) emerged as an organizational and analytical paradigm centered on the use of data, analytical methods, and structured evidence to support institutional decision-making processes (GADE, 2021). Rather than relying exclusively on intuition, personal experience, or reactive approaches, DDDM emphasizes the systematic transformation of raw data into actionable information capable of informing organizational actions, improving situational awareness, and supporting evidence-based governance practices (MAGAKWE, 2025).

Figure 2.4, inspired by the conceptual perspective proposed by (LU et al., 2019), presents a simplified representation of the Data-DDDM lifecycle. The cycle begins with *Data Collection*, in which raw data are gathered from organizational and operational environments, followed by *Data Integration and Preparation*, where heterogeneous data sources are structured, transformed, and prepared for analytical use. Subsequently, *Data Analytics and Processing* activities transform raw data into analytical outputs capable of generating organizational knowledge and insights through the *Knowledge and Insight Generation* stage. These insights support the *Decision Support* process, assisting *Human and Organizational Decision-Making* activities that ultimately lead to *Institutional Actions*. The outcomes of these actions are then subjected to *Feedback, Monitoring and Evaluation* processes, generating new organizational knowledge and enabling a *Continuous Improvement Cycle*. Collectively, the figure illustrates DDDM as a cyclical and iterative organizational process in which data are continuously transformed into actionable insights capable of supporting evidence-based governance and institutional learning.

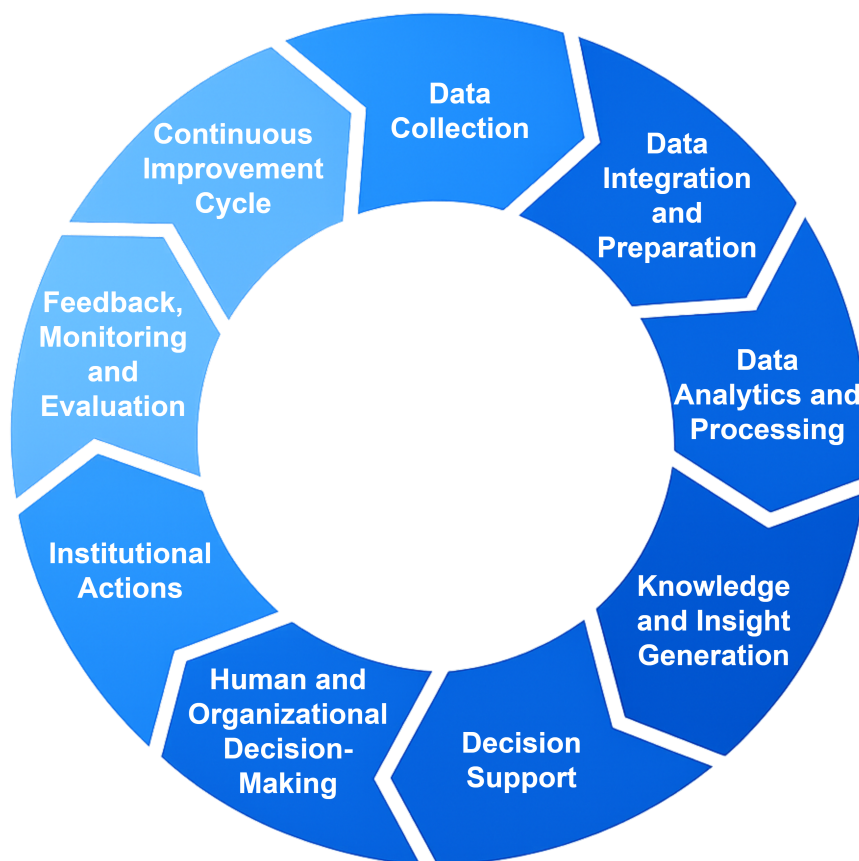


Figure 2.4: Data-Driven Decision-Making Steps

The use of data in public administration has evolved through successive waves of technological maturity, progressing from the automation of bureaucratic processes to the consolidation of data analytics and, more recently, to the adoption of AI enabled decision support systems (BAJRACHARYA, 2024). As Information Systems (IS) became widespread across governmental functions, public agencies expanded their analytical capacity beyond record keeping, incorporating descriptive and diagnostic analytics through dashboards, indicators, and performance monitoring instruments to strengthen managerial decision-making (FREMPONG et al., 2022). More recently, this trajectory has culminated in the increasing adoption of ML and predictive modeling techniques, reflecting the growing institutional capacity to extract patterns from large scale administrative data, forecast outcomes, and anticipate operational or strategic risks (AL-INIZI, 2025). This evolution has positioned data as a strategic asset for governance, enabling more proactive and evidence driven public management.

The increasing availability of digital infrastructures and interoperable datasets has

accelerated the deployment of analytical and AI based systems across diverse public sector domains. In public health, predictive models have been applied to epidemic forecasting (DESAI et al., 2019) and hospital demand estimation (ALMEIDA; CIMA, 2015), while smart city initiatives employ sensor networks and real time analytics to optimize mobility and urban services (RATHORE et al., 2018). These applications illustrate how data intensive systems have become embedded in critical government functions, transforming how public agencies interpret information and respond to complex societal challenges. Importantly, these developments also demonstrate that the public sector increasingly relies on computational methods not only for operational efficiency but also for strategic decision-making under uncertainty.

Beyond improvements in service delivery and administrative management, the growing analytical capacity of governments has enabled new approaches to integrity, oversight, and risk detection. Rather than focusing exclusively on streamlining workflows, AI based systems can analyze vast administrative datasets to identify atypical behaviors, structural irregularities, and patterns indicative of emerging risks (BOUCHETARA; ZEROUTI; ZOUAMBI, 2024). In this context, analytical tools contribute to the prioritization of inspections, the detection of anomalous transactions, and the identification of entities or processes exhibiting elevated risk profiles (ALFIAN; RITCHI; ADRIANTO, 2023). This shift indicates a broader movement toward proactive and data-driven integrity mechanisms in which computational techniques augment professional judgment by revealing latent risk structures that are difficult to observe through traditional auditing practices.

PP constitutes a particularly relevant domain for integrity oriented analytics due to its high economic volume, complex governance structure, and exposure to fraud and collusive behavior. Procurement datasets can be leveraged to detect irregular bidding dynamics (TÓTH; FAZEKAS, et al., 2014), uncover coordinated patterns suggestive of collusion (RODRÍGUEZ et al., 2022), identify suppliers with suspicious histories (MODRUŠAN; RABUZIN; MRŠIC, 2021), and flag price anomalies (POTIN et al., 2023) or contractual configurations associated with elevated fraud risk. These approaches align with similar developments in other oversight intensive domains, such as social benefits administration where models support the identification of abnormal claims or unusual beneficiary behavior (CASTRO RODRIGUES; LIMA; BARBOSA, 2022) and taxation, where analytical systems assist in detecting evasion schemes and prioritizing audit activities (XAVIER et al., 2022). In all these settings, the central contribution of AI and analytics lies in supporting risk screening and prioritization while preserving human accountability in investigative decision-making.

However, the deployment of intelligent systems in the public sector is governed by constraints and responsibilities that differ markedly from those in private organizations. Government agencies operate under mandates of legality, equity, legitimacy, and collective welfare, requiring algorithmic systems to uphold citizens' rights, remain transparent to oversight bodies, and avoid disproportionate harm to vulnerable populations (FINK, 2018). Errors, opacity, or biases in AI systems may compromise service delivery, intensify inequalities, and erode institutional trust, thereby increasing the societal consequences of technical failures (PAGLIERI; COSTUMATO; BONOMI SAVIGNON, 2025). Consequently, the adoption of data driven and AI based decision support in government requires strong safeguards for explainability, fairness, procedural justice, and accountability (TALUKDER, 2025). These distinctive ethical, regulatory, and governance requirements are especially salient in public procurement oversight, where analytical outputs must be both technically robust and institutionally defensible.

2.4 Ethical Aspects and Trustworthy AI

As AI becomes increasingly integrated into government processes, its ethical implications have moved to the forefront of public and academic debate (CATH, 2018; SIGFRIDS et al., 2022). In domains such as PP, where algorithmic decisions can influence the allocation of large scale financial resources and affect institutional integrity, the demand for trustworthy AI is especially pressing (NAGITTA et al., 2022). Ensuring that AI systems respect fundamental rights, operate transparently, and align with democratic values is not merely a technical challenge, but a normative imperative (SHAELOU; RAZMETAeva, 2023; KAN et al., 2024). This section builds on the discussion of explainability and governance to examine how ethical principles can guide the design and deployment of AI in the public sector. Drawing on international frameworks such as the European Commission's Ethics Guidelines for Trustworthy AI (AI, 2019), the following subsections explore how trust can be operationalized in public procurement fraud detection through legal compliance, value alignment, and institutional responsibility.

2.4.1 Defining Trustworthy AI in the Public Sector

The concept of trustworthy AI has emerged as a central reference in the ethical governance of AI, particularly in the public sector, where the stakes of automated decision making are especially high. According to the European Commission's *Ethics Guidelines*

for *Trustworthy AI*, an AI system can only be considered trustworthy if it fulfills three interdependent conditions: it must be *lawful*, complying with all applicable laws and regulations; *ethical*, ensuring adherence to ethical principles and societal values; and *robust*, both from a technical and social perspective. This framework goes beyond mere technical performance to emphasize broader concerns such as legitimacy, accountability, and respect for fundamental rights.

In the context of PP, trust is not only a prerequisite for adoption, but also a public value in itself. Decisions made by AI systems, such as flagging contracts for potential fraud, must be perceived as legitimate by multiple stakeholders, including public managers, oversight institutions, suppliers, and civil society. Unlike the private sector, where trust may be primarily transactional or reputational, in government contexts it is inherently institutional. Citizens expect not only efficiency and innovation, but also fairness, transparency, and legal safeguards.

Furthermore, public trust in AI is fragile and contingent. Studies have shown that algorithmic opacity, perceived unfairness, or lack of redress mechanisms can erode confidence in digital systems and institutions (PURVES; DAVIS, 2022; ARAGANI; ANUMOLU; SELVAKUMAR, 2025; SAMPAIO; FONTES, et al., 2024). For this reason, the implementation of AI in government and especially in sensitive areas like PP must be grounded in ethical and legal commitments that extend beyond accuracy metrics or operational gains. Trustworthy AI in the public sector therefore demands a systemic approach, in which technical development is integrated with institutional design, stakeholder engagement, and normative alignment.

2.4.2 Regulatory and Policy Frameworks for Ethical AI in Government

Over the past years, multiple international organizations have proposed normative frameworks to guide the ethical development and deployment of AI. These documents have become critical references for governments, researchers, and developers seeking to ensure that AI systems operate in accordance with public values, legal principles, and democratic accountability. Among the most influential are the OECD AI Principles (YEUNG, 2020), the UNESCO Recommendation on the Ethics of Artificial Intelligence (KETTEMANN, 2022), and national strategies such as Brazil's Estratégia Brasileira de Inteligência Artificial (BRASIL, 2023). While these initiatives vary in scope and emphasis, they all converge on the need for inclusive, transparent, and human centered AI governance espe-

cially in public sector applications where risks are amplified by institutional power and public impact.

The OECD AI Principles, endorsed by over 30 countries including Brazil, advocate for five complementary values: inclusive growth and sustainable development; human centered values and fairness; transparency and explainability; robustness and safety; and accountability. UNESCO, in turn, emphasizes the ethical implications of AI in education, culture, science, and public service, calling for international cooperation, data sovereignty, and the protection of vulnerable populations. The Brazilian AI Strategy incorporates several of these principles while framing AI as a tool for innovation, competitiveness, and improved public services, with specific attention to fairness, human rights, and transparency. Although these frameworks have enriched the global dialogue on ethical AI, their level of operational detail, particularly regarding public sector implementation — varies considerably.

Given the focus of this thesis on the intersection between ethical principles and the use of AI in public procurement, the *Ethics Guidelines for Trustworthy AI* published by the European Commission were selected as the primary normative foundation. This choice is grounded in three main reasons. First, the EU guidelines offer a comprehensive and actionable set of ethical criteria, structured around a well defined framework that integrates legal, technical, and societal dimensions. Second, the document provides concrete requirements and assessment mechanisms that are particularly well suited for applications in high risk domains such as fraud detection in government contracting. Third, the guidelines reflect a public values oriented perspective that resonates with the accountability and transparency imperatives of digital government. While complementary references from the OECD, UNESCO, and the EBIA are acknowledged throughout the discussion, the EU document was adopted as the central ethical anchor for its clarity, applicability, and relevance to the research problem at hand.

2.4.3 Core Ethical Principles for PP AI fraud detection

The Ethics Guidelines for Trustworthy AI published by the European Commission outline four core ethical principles intended to guide the responsible development and deployment of AI systems: *Respect for Human Autonomy*, *Prevention of Harm*, *Fairness*, and *Explainability* (AI, 2019). *Respect for Human Autonomy* emphasizes the need for meaningful human oversight and control over AI driven decisions, ensuring that individuals retain agency and responsibility. *Prevention of Harm* calls for systems that avoid phys-

ical, psychological, or reputational damage to individuals or society. *Fairness* addresses the obligation to avoid bias, discrimination, or unjust treatment by ensuring equitable outcomes and access. Finally, *Explainability* refers to the capacity of AI systems to be understood, interpreted, and scrutinized by affected stakeholders. While all four principles are relevant to the use of AI in public procurement, this study places particular emphasis on Autonomy and Explainability.

Figure 2.5 presents the four fundamental ethical principles and their definitions. In this figure, the green colored boxes highlight the principles prioritized in this study: Respect for Human Autonomy and Explainability. These principles are emphasized because they are the most critically affected in the context of AI based fraud detection in public procurement. Working with ethical principles in fraud detection presents significant challenges, especially considering the investigative and potentially “criminal” nature of this application. The use of AI in this domain often involves opaque decision-making processes that may impact individuals or organizations without adequate justification or opportunity for contestation. Ensuring fairness and preventing harm becomes complex when identifying irregularities, which can have adverse consequences even without conclusive proof of guilt. Respect for Human Autonomy is essential to ensure that automated systems do not override human judgment, particularly in high stakes government decisions that may result in reputational damage or exclusion from procurement processes. Similarly, Explainability plays a vital role in enabling auditors, public managers, and stakeholders to understand how AI systems reach their conclusions, fostering transparency, legal compliance, and institutional trust. Although other ethical principles such as Fairness and Prevention of Harm are also relevant and should not be overlooked, Autonomy and Explainability are more directly challenged in current AI implementations, which often rely on black-box models with limited interpretability. The European guidelines themselves acknowledge the existence of tensions between ethical principles, such as in the example of “police foresight,” where the need for public safety may conflict with individual rights and privacy. Therefore, this study gives particular emphasis to Respect for Human Autonomy and Explainability, as they represent the ethical foundations most urgently in need of operational strategies to balance effective fraud detection with the obligation to protect individuals from unjust harm and ensure accountability in AI supported auditing processes.

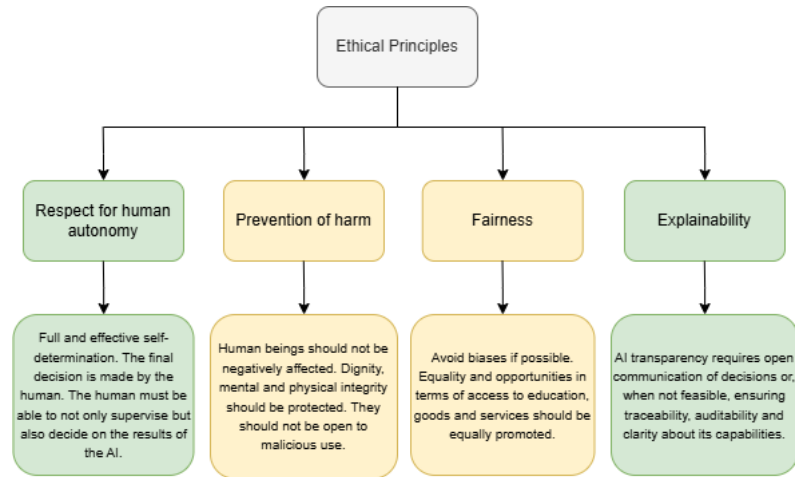


Figure 2.5: Key ethical principles for trustworthy AI in PP fraud detection context (Adapted from Ethics guidelines for trustworthy AI (AI, 2019))

2.5 Data Provenance

Data provenance can be understood not just as a technical mechanism for tracking data transformations, but as an operational enabler of ethical principles in data driven contexts. If the previous section highlighted transparency, accountability, and responsible AI as normative requirements for public sector analytics, provenance provides the structural means through which such principles can be enacted. Provenance data represents the history of data processing by structuring, in a queryable form, the derivation path of a specific data element describing how it was produced, transformed, and acted upon. In the context of this thesis, provenance records the steps and transformations involved in constructing fraud risk indicators. Although provenance has been represented in multiple ways in the literature, the W3C PROV standard (MOREAU; GROTH, 2022) defines a widely adopted data model based on three core components: Entities, Activities, and Agents, along with relationships such as *used* (data consumed by an activity) and *wasGeneratedBy* (data produced by an activity). Within this research, an Entity may correspond to a database tuple or a derived red flag; Activities represent the analytical or transformation steps that operate on these entities; and Agents denote the users or systems responsible for initiating or executing such processes.

The provenance diagrams in Figures 2.6 and 2.7 visually illustrate how the PROV model structures the lifecycle of information through the interaction of Entities, Activities, and Agents. Figure 2.6 presents the canonical PROV data model, highlighting the core relationships that connect these elements. An Entity may be derived from another

entity *wasDerivedFrom*, generated by an activity *wasGeneratedBy*, or used as input in a transformation *used*. An Activity can be informed by previous activities *wasInformedBy* and is associated with responsible actors *wasAssociatedWith*. An Agent, such as a person or system, can be attributed to entities *wasAttributedTo* or act on behalf of another agent *actedOnBehalfOf*. Together, these relationships form a directed graph that makes explicit how data are produced, transformed, and governed.

Figure 2.7 operationalizes this abstract structure through a simplified example: two agents, Simon and Paolo, are associated with an editing activity (edit1), which generates a new document version. The relationships explicitly capture roles (e.g., contributor, editor), document versioning, and the generation process, demonstrating how provenance enables fine grained traceability of responsibility and transformation. By making these relationships machine readable and queryable, provenance diagrams provide a structured representation of accountability: they reveal not only what data exist, but how they came to exist and who was responsible at each stage.

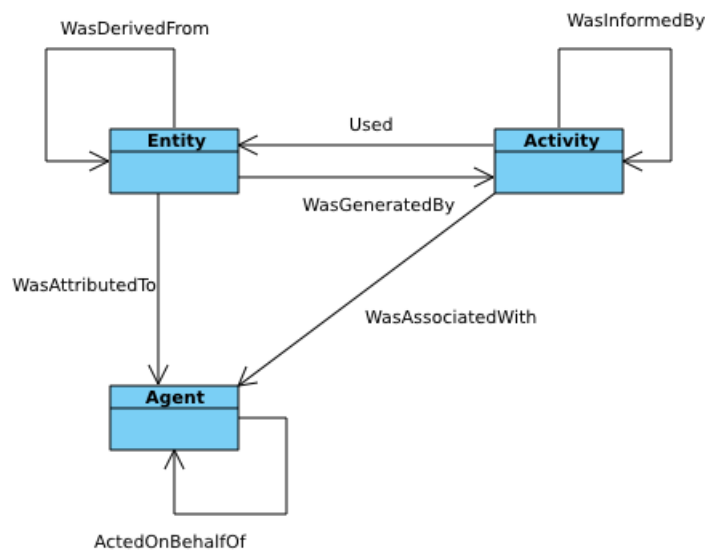


Figure 2.6: Provenance Modeling Using the W3C PROV Standard. Reproduced from PROV-DM

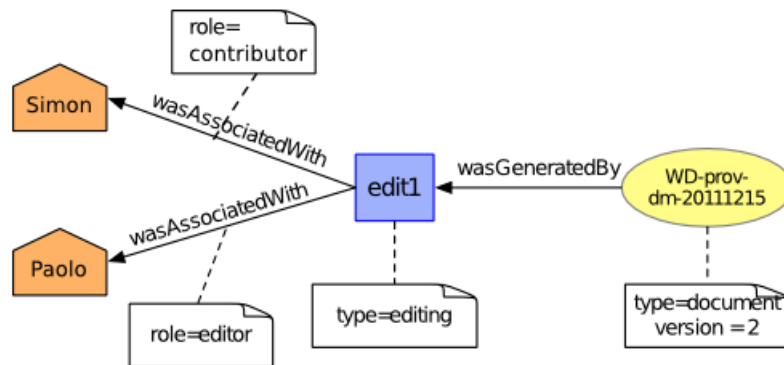


Figure 2.7: Example of a PROV-Based Provenance Graph. Reproduced from PROV-DM

Within IS literature, provenance has been increasingly recognized as a key mechanism for strengthening trust, transparency, and accountability in digital ecosystems (SINGH; COBBE; NORVAL, 2018). Closely aligned with the DAMA-DMBOK framework’s conception of data governance as the exercise of authority and control over data assets (INTERNATIONAL, 2017), provenance operationalizes governance principles by providing verifiable documentation of how data are created, transformed, and used. Its application spans multiple domains, including reproducibility and quality assurance in data science workflows (RUPPRECHT et al., 2020), interoperability and institutional trust (DOUTHIT et al., 2021), and accountability in open data infrastructures (FLOURIS et al., 2012). By making the data lifecycle explicit and linking sources, transformations, and outputs into a coherent chain of evidence (APPELBAUM, 2016), provenance supports the credibility of analytical claims. In the context of public procurement oversight, it enables the traceability of fraud risk indicators, for example, by documenting how data from tax registries, procurement portals, and preprocessing rules are combined to identify whether a newly created company has secured a high value contract. In this sense, provenance extends beyond technical lineage tracking to function as a governance instrument that legitimizes data-driven decision-making and reinforces institutional accountability in digital oversight systems.

2.6 Design Science Research

DSR is a foundational research paradigm in IS concerned with the creation and rigorous evaluation of artifacts designed to solve relevant real world problems (HEVNER et al., 2004). Emerging from early conceptualizations by March et al. (MARCH; SMITH, 1995), and subsequently systematized by Hevner et al. (HEVNER et al., 2004) and Pef-

fers et al. (PEFFERS et al., 2012), DSR positions artifact design as a core scientific contribution, alongside the generation of generalizable knowledge about how artifacts operate within organizational contexts. The paradigm emphasizes the interplay between relevance, addressing practical, socially significant problems and rigor, drawing from established theories, methods, and evidence.

Figure 2.8 illustrates the interplay among the three cycles of Hevner’s DSR framework (HEVNER, 2007). On the left, the Relevance Cycle connects the research to the application environment comprising people, organizational structures, technical systems, and practical problems, informing the requirements that guide artifact development and enabling field testing in real-world contexts. On the right, the Rigor Cycle anchors the research in the knowledge base, drawing on established theories, methods, experience, and prior design artifacts to ensure conceptual grounding and scientific validity. At the center, the Design Cycle iteratively builds, evaluates, and refines the artifact, serving as the dynamic core through which insights from the environment and the knowledge base are continuously integrated. The diagram visually reinforces how these three cycles operate in parallel to produce research outcomes that are both relevant and rigorous.

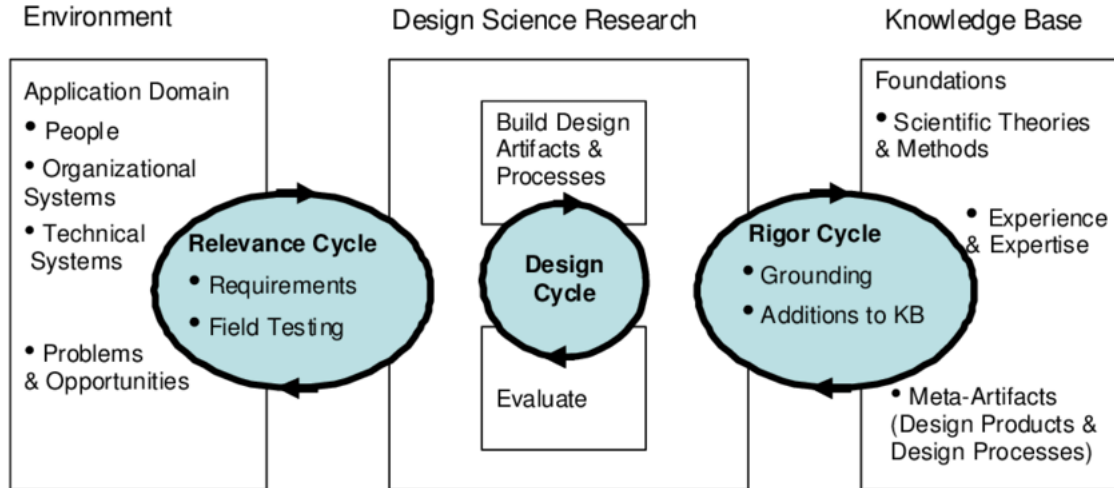


Figure 2.8: Design Science Research Cycles. Reproduced from (HEVNER, 2007)

DSR recognizes multiple types of artifacts, constructs, models, methods, and instantiations, each of which contributes to structuring, solving, or understanding a problem domain. Constructs form the vocabulary and conceptual primitives of the solution space; models capture relationships between concepts; methods provide procedures or algorithms for addressing tasks; and instantiations materialize artifacts in operational systems. Within this thesis, these artifact categories map directly onto the components of the pro-

posed framework. Constructs include the formalization of red flags, provenance entities, and risk related concepts. Models are embodied in the provenance aware framework for risk analysis, which integrates open data, heuristic labeling, and explainability principles. Methods correspond to the processes for deriving, validating, and operationalizing red flags, as well as the pipeline for weak supervision and explainable risk assessment.

Digital government represents a socio technical domain characterized by institutional complexity, heterogeneous stakeholders, legal constraints, and evolving technological possibilities. Problems in this domain, such as fraud analysis in procurement are often ill structured, shaped by political and organizational considerations. DSR is therefore particularly suitable because it integrates scientific rigor with practical relevance, enabling the development of solutions that are both technically sound and institutionally feasible (SCHLIMBACH et al., 2023). DSR facilitates systematic engagement with practitioners, allowing researchers to incorporate domain expertise from auditors and procurement officials into the artifact design. Moreover, the paradigm supports iterative refinement in response to real world constraints, which is essential in contexts requiring transparency, explainability, and value alignment.

2.7 Final Remarks

This chapter established the conceptual and theoretical foundations that sustain the development of this thesis. It examined the evolution of digital government and its transition toward increasingly integrated, data-driven, and citizen centered models, situating public procurement within this broader transformation. By analyzing the structure of PP, the characteristics of procurement data, and the typologies and institutional dynamics of fraud, the chapter clarified the structural complexity and sociotechnical nature of procurement oversight. It further explored the role of data analytics and AI in the public sector, highlighting both their analytical potential and the governance challenges they introduce. The discussion on ethical principles and data provenance reinforced the necessity of transparency, traceability, and accountability in high stakes public decision-support systems.

Finally, the introduction of DSR provided the methodological lens through which these theoretical elements are translated into a structured artifact. By framing the problem as one that requires purposeful design, DSR offers the epistemological and procedural grounding for constructing, instantiating, and evaluating a reference model aligned with

institutional realities. Together, the conceptual foundations and the DSR paradigm ensure that the proposed model is not merely an analytical framework, but a rigorously grounded sociotechnical artifact capable of addressing fraud risk analysis in PP in a responsible, transparent, and institutionally coherent manner.

Chapter 3

Literature Reviews and Expert Knowledge Elicitation

This chapter aims to operationalize the knowledge acquisition and consolidation activities defined in the methodological design of this research. Grounded in the DSR paradigm presented in the methodology chapter, it goes beyond a descriptive literature review by actively supporting problem understanding and artifact design. Within DSR, rigorous artifact development requires systematic engagement with existing scientific knowledge as well as with domain specific expertise. In this sense, the chapter functions as a central component of the rigor cycle, providing the theoretical and empirical foundations necessary to justify the design choices, assumptions, and requirements underlying the proposed framework for fraud risk analysis in public procurement.

To this end, the knowledge acquisition activities defined in the methodological design are operationalized through a combination of Systematic Literature Review (SLR) and expert knowledge elicitation with public auditors. The literature reviews are employed to critically examine prior research on AI based fraud detection and the use of red flags as risk indicators. In parallel, the interviews provide practice oriented insights that allow the findings from the literature to be validated, refined, and contextualized within real-world auditing environments. Together, these activities establish a clear methodological link between the adopted research approach and the subsequent design and evaluation of the proposed artifact, ensuring both theoretical rigor and institutional relevance.

3.1 SLR Protocol and Review Strategy

To ensure methodological consistency and avoid redundancy across the different SLR conducted in this research, a unified review protocol was adopted. In line with established guidelines for evidence-based software engineering and information systems research (KITCHENHAM, 2004), all reviews followed a common SLR structure composed of three main phases: planning, study selection, and analysis. This shared protocol allows the individual reviews to be interpreted as complementary components of a coherent knowledge acquisition process rather than as isolated efforts. By establishing a common methodological foundation, the protocol enhances transparency, reproducibility, and comparability across the reviews.

The literature search was conducted using major scientific databases that index peer-reviewed research in computer science, information systems, and public administration, including Scopus¹, IEEE Xplore², and the ACM Digital Library³. These sources were selected to capture interdisciplinary contributions related to AI, digital government, auditing, and public sector oversight. Only studies published in English and subjected to peer review were considered. The temporal scope of the searches covered publications up to 2026, reflecting the period in which data-driven and AI-supported approaches in the public sector have substantially evolved.

Study selection followed a multi-stage screening process. Initially, titles and abstracts were assessed against review-specific inclusion and exclusion criteria, derived from the corresponding PICOC frameworks (WOHLIN et al., 2012) and tailored to the analytical focus of each systematic literature review. These criteria are explicitly detailed in the respective sections of each SLR. In the subsequent stage, full-text screening was conducted to confirm relevance, resolve ambiguities, and ensure alignment with the specific research questions guiding each review. Following study selection, a qualitative analysis was performed to synthesize the findings across the included studies. This analysis employed iterative coding and thematic synthesis to identify recurring patterns, limitations, and research gaps, which directly informed the comparative analysis across reviews and supported the derivation of design implications presented in this work.

¹<https://www.scopus.com/home.uri>

²<https://ieeexplore.ieee.org/Xplore/home.jsp>

³<https://dl.acm.org/>

3.2 SLR I — Artificial Intelligence for Fraud Detection in Public Procurement

The purpose of this review was to comprehensively identify and analyze studies that investigate the application of AI to fraud detection in public procurement. During the planning phase, a review protocol was defined, specifying the research questions, search strategy, and inclusion and exclusion criteria. The protocol was designed to ensure a systematic and reproducible identification of relevant studies. SLR I was guided by one research question: **RQ1:***How has artificial intelligence been applied to fraud detection in public procurement?*

The search strategy was designed to encompass three core domains of interest: Machine Learning, Fraud, and Government Data, with particular attention to PP related contexts. Accordingly, the following search string was defined: *("Fraud" OR "Collusion" OR "Corruption") AND ("Machine Learning" OR "Artificial Intelligence" OR "Artificial Neural Networks" OR "Deep Learning") AND ("Public Government" OR "Digital Government" OR "Electronic Government" OR "Government" OR "Public Procurement" OR "e-gov")*. The term "Artificial Intelligence" was intentionally included to generalize and capture the broader spectrum of machine learning techniques. Likewise, the set of terms ("Public Government" OR "Digital Government" OR "Electronic Government" OR "Government" OR "Public Procurement" OR "e-gov") was deliberately expanded beyond the specific expression "public procurement" in order to transcend domain-specific terminology limitations. Many studies may rely on government datasets that include procurement-related information without explicitly labeling their context as PP.

The selection criteria were divided into inclusion and exclusion criteria. The inclusion criteria were: (I1:) Publications that use AI methods to detect fraud in public procurements; (I2:) Systematic Literature Reviews that address the researched topic. Six exclusion criteria were (E1:) Publications that use AI methods to detect fraud outside the scope of PP; (E2:) Publications that have absolutely no correlation with the topic; (E3:) Publications that do not have any AI method involved; (E4:) The publication must be a complete article. Short articles, books, letters, notes and patents are excluded; (E5:) Publications must be in English; (E6:) Publications must be unique. If a publication is repeated, other copies of that publication will be deleted.

The systematic search strategy resulted in an initial set of studies retrieved from multiple scientific databases. A total of 435 records were identified through Scopus, 313

through IEEE Xplore, and 411 through the ACM Digital Library, a total of 1159. After the removal of duplicates, 1069 studies remained for full-text assessment. Following full-text screening, a final corpus of 38 primary studies was retained for qualitative synthesis. This set of studies constitutes the analytical basis for answering the research questions of SLR I and reflects the current body of peer-reviewed research on the application of artificial intelligence to fraud detection in public procurement. Figure 3.1 summarizes this selection process by depicting the flow of studies across the identification, screening, and inclusion phases of the review.

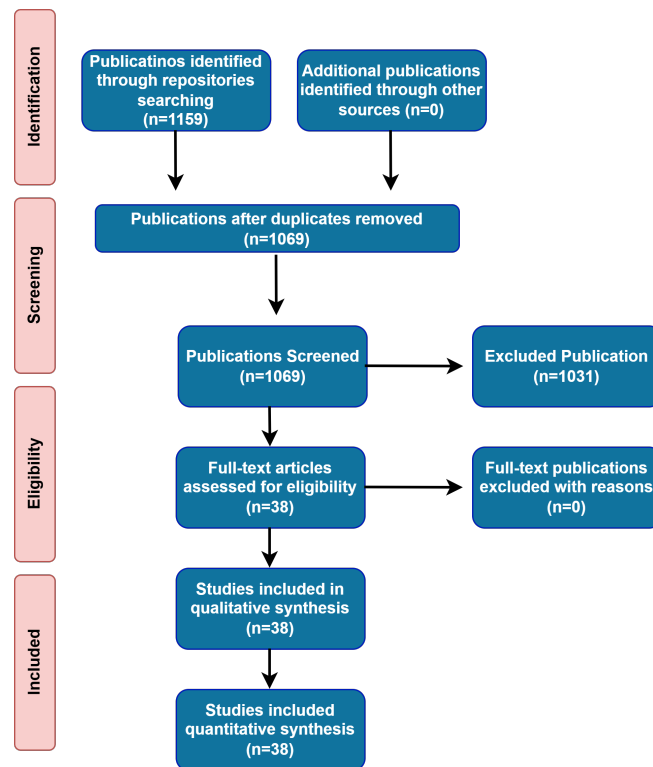


Figure 3.1: Information flow through the steps of the review using PRISMA Flow Diagram - SLR I (Adapted from Moher et al (MOHER et al., 2009))

The reviewed studies reveal a diverse landscape of AI and ML approaches applied to fraud detection in PP. As summarized in Table 3.1, Natural Language Processing (NLP) emerges as the most frequently employed category, reflecting the relevance of textual analysis in procurement documents, tender specifications, and legal records to uncover irregularities, favoritism, and corruption related signals. Supervised learning and rule guided ML approaches follow closely, indicating a significant reliance on predictive modeling. Unsupervised learning techniques also play a prominent role, particularly in anomaly detection scenarios where reliable ground-truth fraud labels are unavailable. Hybrid approaches demonstrate an increasing tendency toward methodological integration,

combining multiple paradigms, such as rules, predictive models, and anomaly detection, within broader analytical pipelines. In contrast, semi-supervised learning appears only marginally in the reviewed corpus, and graph/network-based methods, although relevant for detecting collusive structures, are less frequently adopted. Overall, the methodological distribution reflects a field that balances document centric analysis, rule operationalization, and predictive modeling, while still contending with structural data and labeling limitations inherent to PP environments.

Table 3.1: AI Methods Categories Applied to Fraud Detection in Public Procurement

Method	Publication	Total
Unsupervised Learning	(MOHD; NOHUDDIN, 2021), (CHORNYI; SHILO; LEBEDIEVA-DYCHKO, 2025), (NIESSEN; PACIELLO; FERNANDEZ, 2020), (DOMASHOVA; KRIPAK, 2021), (DOMINGOS et al., 2016), (SOYLU et al., 2022)	6
Supervised Learning	(DEMETER et al., 2025), (TAS, 2024), (FUERTES et al., 2025), (SAMPAIO; FONTES, et al., 2024), (GALLEGO; RIVERO; MARTÍNEZ, 2021), (NAI; MEO, et al., 2023), (AVDASHEVA; KORNEEVA; YUSUPOVA, 2025)	7
Semi Supervised Learning	(TAS, 2022)	1
NLP	(TORRES-BERRU; LOPEZ-BATISTA; ZHINGRE, 2023), (NAI; FATIMA, et al., 2023), (GOMES; COLAÇO, 2022), (ULLOA et al., 2025), (LIMA et al., 2023), (RABUZIN; MODRUSAN, 2019), (MAVIDIS; FOLINAS; SKIADAS, 2025), (TORRES-BERRU; LÓPEZ BATISTA, 2022)	8
Hybrid	(VELASCO et al., 2021), (LYRA et al., 2022), (BRANDÃO et al., 2024), (NAI; SULIS; MEO, et al., 2022), (RIYAD et al., 2024), (TORRES BERRU et al., 2020)	6
Rule Guided ML	(PURWANTO; EMANUEL, 2020), (RACHMAT et al., 2025), (MENKE; GOMES; XAVIER, 2024), (DELLO; YOSHIDA, 2017), (KAZBEKOVA et al., 2025), (ALWASSITI; MORTEZA, 2025), (MICHAEL, 2024)	7
Graph/Network Based Methods	(CRUZ et al., 2023), (MUÑOZ-CANCINO; RÍOS, 2025), (POMPEU; FILHO, 2024)	3

The reviewed studies draw upon a heterogeneous set of data sources that mirror the operational complexity of PP systems. As summarized in Table 3.2, the dominant data backbone across the literature consists of structured transactional procurement data extracted primarily from open government procurement portals and standardized platforms, encompassing contract values, bidding activity, procedural timelines, competition metrics, supplier attributes, and award conditions, which are extensively leveraged for anomaly detection, risk modeling, and early warning systems. A growing body of work enriches these numerical records with relational and network data, explicitly modeling bidder–tender interactions, co-participation patterns, ownership links, and institutional connections to uncover collusive behavior and coordinated fraud schemes. In parallel, a substantial subset of studies employs textual and document-based data obtained from tender documentation, contract clauses, technical specifications, invoices, and administrative communications, applying natural language processing techniques to identify favoritism, inconsistencies, and corruption signals embedded in legal and procedural language.

While the vast majority of empirical contributions rely on open government procurement databases as their primary data source, as evidenced by the distribution of studies reported in Table 3.2, only a limited number of works incorporate labeled enforcement and outcome data, such as court confirmed collusion cases, regulatory sanctions, or audit outcomes, to support supervised learning. This structural scarcity of verified fraud

labels has consequently driven widespread reliance on unlabeled datasets, proxy indicators, and weakly supervised approaches. Overall, the data landscape evidenced in this review highlights both the central role of open procurement data ecosystems in enabling AI based fraud detection and the institutional constraints associated with restricted access to enforcement records, underscoring the importance of integrated, multi-source data infrastructures for robust and accountable analytical frameworks.

Table 3.2: Classification of Data Sources in Public Procurement Fraud Detection Research

Source Type	Publication	Total
Transactional Procurement Data	(CHORNYI; SHILO; LEBEDIEVA-DYCHKO, 2025), (DOMASHOVA; KRIPAK, 2021), (NIESSEN; PACIELLO; FERNANDEZ, 2020), (SOYLU et al., 2022), (DOMINGOS et al., 2016), (SAMPAIO; FONTES, et al., 2024), (FUERTES et al., 2025), (VELASCO et al., 2021), (LYRA et al., 2022), (NAI; SULIS; MEO, et al., 2022), (RIYAD et al., 2024), (TORRES BERRU et al., 2020), (PURWANTO; EMANUEL, 2020), (MENKE; GOMES; XAVIER, 2024), (DELLO; YOSHIDA, 2017), (KAZBEKOVA et al., 2025), (ALWASSITI; MORTEZA, 2025), (MICHAEL, 2024)	18
Relational / Network Data	(MOHD; NOHUDDIN, 2021), (CRUZ et al., 2023), (MUÑOZ-CANCINO; RÍOS, 2025), (POMPEU; FILHO, 2024)	4
Textual and Document Data	(TORRES-BERRU; LOPEZ-BATISTA; ZHINGRE, 2023), (NAI; FATIMA, et al., 2023), (GOMES; COLAÇO, 2022), (ULLOA et al., 2025), (LIMA et al., 2023), (RABUZIN; MODRUSAN, 2019), (MAVIDIS; FOLINAS; SKIADAS, 2025), (TORRES-BERRU; LÓPEZ BATISTA, 2022) (BRANDÃO et al., 2024)	9
Labeled Enforcement and Outcome Data	(TAS, 2024), (DEMETER et al., 2025), (GALLEGO; RIVERO; MARTÍNEZ, 2021), (NAI; MEO, et al., 2023), (AVDASHEVA; KORNEEVA; YUSUPOVA, 2025), (TAS, 2022), (RACHMAT et al., 2025)	7

The reviewed literature addresses a diverse yet structured set of fraudulent behaviors within PP systems. As synthesized in Table 3.3, a dominant research stream focuses on collusion and cartel formation, reflecting the prevalence of coordinated bidding schemes and competition suppression as central corruption mechanisms. A second prominent group of studies targets favoritism and bias, particularly in contract awarding processes where preferential treatment can be embedded in both structured decisions and textual documentation. Several contributions examine overpricing and inefficiency, leveraging anomaly detection and risk modeling to identify abnormal financial patterns indicative of waste or fraud. Issues related to procedural manipulation, such as tailored specifications, limited competition windows, and irregular tender designs, are also extensively investigated through red-flag systems and process analytics. Finally, a smaller yet significant subset of works concentrates on malfeasance and contract abuse in post-award execution, including contract breaches, performance deviations, and misuse of public funds.

Table 3.3: Fraud Types Addressed Across Reviewed Studies

Fraud Type	Publication	Total
Collusion and cartels	(MOHD; NOHUDDIN, 2021), (TAS, 2024), (DEMETER et al., 2025), (AVDASHEVA; KORNEEVA; YUSUPOVA, 2025), (MICHAEL, 2024), (CRUZ et al., 2023), (MUÑOZ-CANCINO; RÍOS, 2025), (POMPEU; FILHO, 2024)	8
Favoritism and bias	(TORRES-BERRU; LOPEZ-BATISTA; ZHINGRE, 2023), (TORRES-BERRU; LÓPEZ BATISTA, 2022), (MUÑOZ-CANCINO; RÍOS, 2025)	3
Overpricing and inefficiency	(CHORNYI; SHILO; LEBEDIEVA-DYCHKO, 2025), (DOMINGOS et al., 2016), (NIESSEN; PACIELLO; FERNANDEZ, 2020), (RABUZIN; MODRUSAN, 2019), (KAZBEKOVA et al., 2025), (DOMASHOVA; KRIPAK, 2021)	6
Procedural manipulation	(SOYLU et al., 2022), (LIMA et al., 2023), (GOMES; COLAÇO, 2022), (PURWANTO; EMANUEL, 2020), (DELLO; YOSHIDA, 2017), (NAI; FATIMA, et al., 2023)	6
Malfeasance and contract abuse	(GALLEGO; RIVERO; MARTÍNEZ, 2021), (RACHMAT et al., 2025), (MENKE; GOMES; XAVIER, 2024)	3
Multi-risk corruption	(FUERTES et al., 2025), (TAS, 2022), (ULLOA et al., 2025), (VELASCO et al., 2021), (LYRA et al., 2022), (NAI; SULIS; MEO, et al., 2022), (RIYAD et al., 2024), (TORRES BERRU et al., 2020), (BRANDÃO et al., 2024), (MAVIDIS; FOLINAS; SKIADAS, 2025), (ALWASSITI; MORTEZA, 2025)	12

Beyond the typology of fraudulent behaviors, the reviewed studies can also be orga-

nized according to the stages of the procurement lifecycle in which analytical interventions are applied. As summarized in Table 3.4, the tendering and bidding stage emerges as the primary focus of AI based detection efforts, largely driven by the observability of collusion patterns and competition anomalies at this phase. The award and contracting stage is frequently examined in studies addressing favoritism, bias, and procedural inconsistencies in winner selection. The pre-tender stage, though less explored, is increasingly recognized as critical for identifying manipulated specifications and early risk indicators. Finally, post-award and execution-phase monitoring remains comparatively underrepresented, despite its relevance for detecting malfeasance, contract breaches, and financial misuse. This lifecycle-based distribution underscores a strong research emphasis on early-stage risk detection while revealing important gaps in continuous contract oversight.

Table 3.4: Procurement Stages Targeted Across Reviewed Studies

Procurement Stage	Publication	Total
Pre-tender stage	(SOYLU et al., 2022), (LIMA et al., 2023), (FUERTES et al., 2025)	3
Tendering and bidding stage	(MOHD; NOHUDDIN, 2021), (TAS, 2024), (DEMETER et al., 2025), (AVDASHEVA; KORNEEVA; YUSUPOVA, 2025), (MICHAEL, 2024), (CRUZ et al., 2023), (POMPEU; FILHO, 2024), (PURWANTO; EMANUEL, 2020), (RABUZIN; MODRUSAN, 2019), (DOMASHOVA; KRIPAK, 2021), (SAMPAIO; FONTES, et al., 2024), (DELLO; YOSHIDA, 2017)	12
Award and contracting stage	(TORRES-BERRU; LÓPEZ-BATISTA; ZHINGRE, 2023), (GOMES; COLAÇO, 2022), (NAI; FATIMA, et al., 2023), (TORRES-BERRU; LÓPEZ BATISTA, 2022), (MUÑOZ-CANCINO; RÍOS, 2025), (NAI; MEO, et al., 2023)	6
Post-award and execution stage	(DOMINGOS et al., 2016), (GALLEGO; RIVERO; MARTÍNEZ, 2021), (RACHMAT et al., 2025), (MENKE; GOMES; XAVIER, 2024)	4
Multi-stage / cross-stage	(CHORNYI; SHILO; LEBEDIEVA-DYCHKO, 2025), (NIESSEN; PACIELLO; FERNANDEZ, 2020), (TAS, 2022), (ULLOA et al., 2025), (VELASCO et al., 2021), (LYRA et al., 2022), (BRANDÃO et al., 2024), (NAI; SULIS; MEO, et al., 2022), (RIYAD et al., 2024), (TORRES BERRU et al., 2020), (MAVIDIS; FOLINAS; SKIADAS, 2025), (KAZBEKOVA et al., 2025), (ALWASSITI; MORTEZA, 2025)	13

3.3 SLR II — Red Flags and Risk Indicators in Public Procurement

The purpose of this second systematic literature review was to comprehensively identify and analyze studies that investigate the use of red flags, fraud indicators, and risk signals in the context of PP. While SLR I focused on AI based and ML approaches, this review was intentionally designed to capture a broader set of contributions that do not necessarily rely on AI techniques. In particular, SLR II aims to encompass rule based, heuristic, expert driven, and indicator based approaches, which remain widely used in procurement oversight and auditing practices. This distinction was necessary to ensure that relevant non AI methodologies, often foundational to risk assessment and institutional monitoring, were not excluded from the analysis.

During the planning phase, a review protocol was defined, specifying the research question, search strategy, and inclusion and exclusion criteria. The protocol was designed to ensure a systematic, transparent, and reproducible identification of relevant studies. SLR II was guided by the following research question: **RQ2: How are red flags and**

risk indicators defined and applied to identify fraud risks in public procurement?

The search strategy was structured to reflect this broader analytical scope. Accordingly, the following search string was defined: (*"Red Flags" OR "Fraud indicators" OR "Risk indicators" OR "Risk signals"*) AND (*"Public Procurement" OR "Electronic Government" OR "Government" OR "Public Government" OR "e-gov"*). Unlike SLR I, this search strategy deliberately excluded terms related to AI and ML in order to capture studies grounded in heuristic reasoning, rule based frameworks, audit manuals, regulatory practices, and expert-defined indicators. This approach allowed the review to map how fraud risks are traditionally identified and operationalized in public procurement, independently of automated or data-driven modeling techniques.

The study selection process was governed by clearly defined inclusion and exclusion criteria. The inclusion criteria were: (I1) publications that define, analyze, or operationalize red flags, fraud indicators, or risk signals in PP; (I2) systematic literature reviews related to fraud indicators or procurement risk assessment; and (I3) publications that contribute conceptually or empirically to the understanding of procurement fraud risks. The exclusion criteria were: (E1) publications addressing fraud indicators outside the public procurement domain; (E2) publications with no substantive relation to fraud risk identification; (E3) publications focusing exclusively on AI or ML techniques without explicit discussion of indicators or red flags; (E4) incomplete publications such as short papers, editorials, books, letters, notes, or patents; (E5) publications not written in English; and (E6) duplicate records.

The systematic search strategy resulted in an initial set of studies retrieved from multiple scientific databases. Following the identification phase, duplicate records were removed and the remaining studies were subjected to title, abstract, and full-text screening according to the defined criteria. After this screening process, a final corpus of primary studies was retained for qualitative synthesis. This set of studies constitutes the analytical basis for SLR II and reflects the state of the art in the definition and application of red flags and risk indicators in public procurement. Figure 3.2 summarizes the study selection process, illustrating the flow of records across the identification, screening, and inclusion phases of the review.

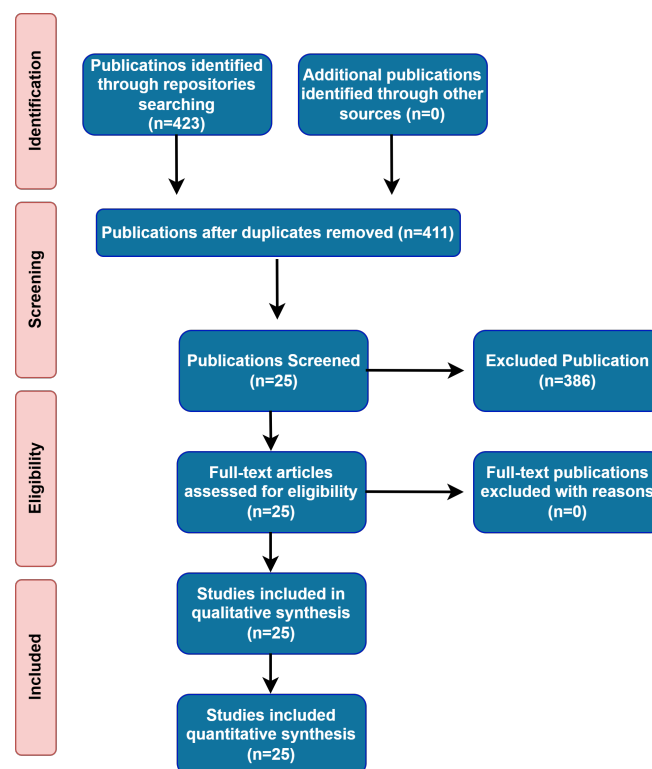


Figure 3.2: Information flow through the steps of the review using PRISMA Flow Diagram - SLR II (Adapted from Moher et al (MOHER et al., 2009))

The reviewed studies reveal a diverse yet conceptually coherent set of red flags and risk indicators employed to identify fraud risks in public procurement. As summarized in Table 3.5, the literature consistently organizes these indicators around recurring dimensions of risk that capture different facets of the procurement process. Importantly, these dimensions are not treated as mutually exclusive, and several studies simultaneously adopt multiple types of red flags in order to capture complementary manifestations of risk. A prominent group of studies emphasizes competition-related red flags, which signal potential restrictions of competitive pressure through patterns such as single bidding, low bidder turnout, or repeated participation of the same suppliers. These signals are frequently combined with procedural red flags, which capture deviations in the formal conduct of procurement processes, including the excessive use of non-competitive procedures, atypical timelines, or fragmented contracting practices.

Another recurrent dimension concerns transparency and information-related red flags, which arise from missing, incomplete, or opaque procurement data and are commonly associated with reduced accountability and oversight capacity. Many studies incorporate these indicators alongside other categories, reflecting the interdependence between information availability and the detection of irregularities. In parallel, a substantial body of

work employs economic and financial red flags to identify anomalous pricing patterns, cost overruns, frequent contract amendments, or discrepancies between estimated and awarded values, treating these signals as proxies for inefficiency or rent extraction. Beyond contract-level attributes, several studies also emphasize behavioral and relational red flags, capturing persistent interaction patterns between contracting authorities and suppliers, concentration of awards, and network structures suggestive of favoritism or collusion. Finally, a smaller but significant stream of the literature incorporates structural and contextual red flags, which account for sectoral, institutional, temporal, or territorial conditions—such as emergency periods or historically vulnerable sectors—that systematically increase exposure to corruption risk and are often used to contextualize or weight other indicators.

Taken together, the typology presented in Table 3.5 illustrates that red flags in PP are predominantly conceived as non conclusive, risk based signals intended to support screening, prioritization, and investigative decision making. Rather than functioning as direct evidence of wrongdoing, these indicators are typically deployed in combination, guiding auditors and oversight bodies toward areas where further scrutiny is warranted. This multiplicity of signals reinforces the role of red flags as interpretative instruments within broader decision support and risk based oversight frameworks, rather than as standalone determinants of fraudulent behavior.

Table 3.5: Typology of Red Flags and Risk Indicators in Public Procurement

Red Flag Category	Indicators Examples	Procurement Phase	Publications
Competition	Single-bid tenders; Low number of bidders; Recurrent participation or winning by the same suppliers; Lack of effective competition despite open procedures	Tendering; Award	(LISCIANDRA; MILANI; MILLEMACI, 2022), (FAZEKAS; TÓTH; KING, 2016), (NIESSEN; PACIELLO; FERNANDEZ, 2020), (FERWERDA; DELEANU; UNGER, 2017), (DECAROLIS; GIORGANTONIO, 2022), (TÓTH; HAJDU, 2025), (DAVIS; MENDOZA; YAP, 2024), (FAZEKAS; TÓTH; ABDOU, et al., 2024), (TÁTRAI; NÉMETH, 2018), (GNALDI; DEL SARTO, 2024), (BRANDÃO et al., 2024), (FUERTES et al., 2025), (MARTÍNEZ-PLUMED et al., 2018), (FAZEKAS; KOCSIS, 2020), (MARCHESSAULT; KLUTTZ; FERNÁNDEZ, 2025), (MOHD; LIAB, 2025)
Procedure	Excessive use of non-competitive or exceptional procedures; Repeated contract splitting Unjustified use of accelerated timelines; Irregular sequencing or omission of mandatory procedural steps	Planning; Tendering; Award	(LISCIANDRA; MILANI; MILLEMACI, 2022), (FAZEKAS; TÓTH; KING, 2016), (FERWERDA; DELEANU; UNGER, 2017), (DECAROLIS; GIORGANTONIO, 2022), (TÓTH; HAJDU, 2025), (GNALDI; DEL SARTO, 2024), (TÁTRAI; NÉMETH, 2018), (BRANDÃO et al., 2024), (FUERTES et al., 2025), (OOSTHOEK, 2020), (MARTÍNEZ-PLUMED et al., 2018), (TISHCHENKO, 2016), (MOHD; LIAB, 2025)
Transparency and Information	Missing or incomplete procurement records; Late or selective publication of tender or award information; Lack of disclosure of evaluation criteria or contract amendments; Poor data standardization across procurement platforms	Tendering; Award; Contract execution	(NIESSEN; PACIELLO; FERNANDEZ, 2020), (ULLOA et al., 2025), (FERWERDA; DELEANU; UNGER, 2017), (DECAROLIS; GIORGANTONIO, 2022), (FAZEKAS; ABDOU, et al., 2022), (FAZEKAS; TÓTH; ABDOU, et al., 2024), (TÁTRAI; NÉMETH, 2018), (OOSTHOEK, 2020), (BRANDÃO et al., 2024), (MARCHESSAULT; KLUTTZ; FERNÁNDEZ, 2025)
Economic and Financial Issues	Significant price deviations from benchmarks or estimates; Cost overruns and frequent contract amendments High volume of change orders; Discrepancies between planned, awarded, and executed values	Award; Contract execution	(LISCIANDRA; MILANI; MILLEMACI, 2022), (FAZEKAS; TÓTH; KING, 2016), (FERWERDA; DELEANU; UNGER, 2017), (DECAROLIS; GIORGANTONIO, 2022), (TÓTH; HAJDU, 2025), (TAHMINA; NAIMA, 2016), (GNALDI; DEL SARTO, 2024), (FUERTES et al., 2025), (SELIM; YOUSEF; HAGAG, 2019), (MARTÍNEZ-PLUMED et al., 2018), (TISHCHENKO, 2016), (FAZEKAS; KOCSIS, 2020)
Behavior/Relational Issues	Persistent buyer-supplier relationships over time; High concentration of awards among a small group of firms; Co-bidding or network patterns suggestive of collusion; Rotational winning patterns among suppliers	Tendering; Award; Cross-contract / longitudinal analysis	(FAZEKAS; WACHS, 2020), (DECAROLIS; GIORGANTONIO, 2022), (DAVIS; MENDOZA; YAP, 2024), (WESTERSKI et al., 2021), (MARTÍNEZ-PLUMED et al., 2018), (TISHCHENKO, 2016), (MOHD; LIAB, 2025)
Structure/Contextual Issues	Procurement conducted during emergency or crisis periods; Sector-specific vulnerabilities; Institutional capacity constraints; Regional or organizational historical exposure to corruption risk	Cross-phase; Contextual to the entire procurement cycle	(LISCIANDRA; MILANI; MILLEMACI, 2022), (FAZEKAS; TÓTH; KING, 2016), (FAZEKAS; WACHS, 2020), (TÓTH; HAJDU, 2025), (FAZEKAS; ABDOU, et al., 2022), (FAZEKAS; TÓTH; ABDOU, et al., 2024), (GNALDI; DEL SARTO, 2024), (OOSTHOEK, 2020), (MODRUŠAN; RABUZIN; MRŠIĆ, 2021), (SELIM; YOUSEF; HAGAG, 2019), (FAZEKAS; KOCSIS, 2020), (MARCHESSAULT; KLUTTZ; FERNÁNDEZ, 2025)

A subset of four studies—(NIESSEN; PACIELLO; FERNANDEZ, 2020), (BRANDÃO

et al., 2024), (FUERTES et al., 2025), and (ULLOA et al., 2025)—appeared in both SLR I and SLR II, reflecting their integrative role in the literature. These works bridge methodological approaches based on AI and ML with the conceptual and operational formulation of red flags and risk indicators. In particular, three of these studies employ data-driven models—such as anomaly detection and supervised risk prediction—while simultaneously relying on structured procurement indicators that function as red flags. The fourth study contributes by proposing a generalized data framework that enables the systematic operationalization of such indicators. Their presence in both reviews is therefore intentional and analytically justified, as they connect computational modeling strategies with the risk-based logic that underpins red flag-driven oversight in public procurement.

3.4 Synthesis of SLR Findings and Research Challenges

This section synthesizes the findings derived from the SLR and complementary analytical extractions conducted throughout this chapter in order to critically assess the current state of research on fraud risk analysis in PP. Rather than reiterating isolated results, the objective is to examine how the identified streams, AI based detection approaches and red flag and risk indicator methodologies, interrelate and where they collectively remain insufficient. Although each stream contributes important insights into specific dimensions of the problem, none offers an integrated perspective capable of reconciling analytical performance with institutional interpretability and accountability. Taken together, the literature reveals a fragmented research landscape in which predictive capability, transparency, and governance mechanisms are typically developed in isolation rather than embedded within a coherent and unified framework.

3.4.1 Strengths and Limitations of AI based Approaches

The literature reviewed in SLR I demonstrates that AI based approaches significantly expand the analytical capacity of fraud risk assessment in PP. ML techniques enable large scale processing of transactional data, allowing the identification of patterns that would be infeasible to detect through manual auditing. Unsupervised anomaly detection models uncover statistical deviations in bidding behavior, pricing structures, and contract execution, while network and graph-based analytics reveal relational patterns suggestive of collusion or concentrated award structures. Supervised models further support early-warning systems capable of estimating corruption risk before contract execution, thereby enhancing

preventive oversight. Collectively, these methods provide scalability, pattern discovery, and predictive capability that substantially exceed traditional rule-based screening.

However, these strengths are accompanied by structural limitations. Many AI based models operate as opaque or semi opaque systems, limiting interpretability beyond technical explanations of model behavior. Their outputs often rely on proxy variables rather than verified instances of corruption, reinforcing epistemic uncertainty in risk classification. Moreover, these approaches remain weakly integrated with institutional decision making processes, offering analytical outputs without systematically embedding them into governance frameworks or accountability mechanisms. Their performance is also highly sensitive to data quality, completeness, and standardization, conditions that are frequently inconsistent across PP ecosystems. As a result, while AI based methods are powerful tools for pattern discovery and risk estimation, they remain institutionally fragile when deployed without complementary mechanisms that ensure interpretability, traceability, and governance alignment.

3.4.2 Red Flags Conceptual Robustness and Fragmentation

The literature reviewed in SLR II highlights the central role of red flags and risk indicators as institutionally grounded instruments for fraud risk assessment in PP. Unlike purely data driven models, red flags are typically rooted in normative frameworks, audit practice, and regulatory standards, which grants them high interpretability and institutional legitimacy. Their logic is transparent: each indicator represents a clearly defined signal associated with elevated corruption risk, facilitating communication among auditors, oversight bodies, and policymakers. This conceptual clarity makes red flags particularly suitable for risk-based screening, prioritization of audits, and accountability oriented reporting.

Despite these strengths, the operational landscape of red flags remains fragmented. The literature reveals considerable methodological variability in how indicators are defined, measured, and combined, with limited formal systematization across jurisdictions. There is no widely adopted international standard governing their construction, weighting, or validation. In many cases, red flags are applied through manual screening or heuristic rules, relying heavily on human judgment rather than systematic analytical integration. Even when formalized into indices, they are often detached from advanced analytical models, limiting their scalability and adaptability to complex datasets. As a consequence, detection patterns frequently remain embedded within institutional expertise rather than being structurally encoded into reproducible analytical pipelines. Red

flags therefore remain explainable and institutionally meaningful instruments, yet analytically under integrated and structurally fragmented within contemporary fraud risk analytics.

3.4.3 Structural Fragmentation and Emerging Research Challenges

The structural fragmentation identified across the literature streams gives rise to a set of interrelated research challenges that directly inform the design requirements of the proposed reference model.

- **RC1 — Integration of Analytical and Institutional Logics:** How can AI driven analytical models be systematically integrated with institutionally grounded red flags and risk indicators within a unified risk assessment architecture? Addressing this challenge requires an engine capable of combining data driven pattern discovery with normative, rule based signals, ensuring that computational detection mechanisms remain aligned with established oversight practices.
- **RC2 — Decision Level Explainability and Traceability:** How can explainability be extended beyond model-level interpretation toward decision level traceability that documents how risk signals are generated, combined, and transformed into actionable outputs? This challenge calls for mechanisms that connect model outputs, red flags, and subsequent audit prioritization steps within a transparent and auditable decision layer.
- **RC3 — Embedded Provenance and Accountability Mechanisms:** How can provenance modeling be embedded directly into fraud risk analytics pipelines to formally represent entities, activities, and agents involved in data transformation and risk scoring? Addressing this issue requires integrating lineage tracking and governance controls not only at the data layer but throughout the analytical workflow.
- **RC4 — Scalability with Governance Alignment:** How can scalable fraud detection mechanisms be deployed without compromising strategic control, institutional oversight, and human accountability? This challenge highlights the need for governance structures capable of supervising model operation, recalibration, and validation across different procurement contexts.
- **RC5 — Operationalization of Risk Based Oversight:** How can fraud risk analysis be operationalized as a structured, end to end decision support process

that links data ingestion, risk computation, explanation, prioritization, and audit feedback loops? This challenge points to the necessity of a layered architecture in which analytical, ethical, and governance components are systematically interconnected rather than loosely coupled.

3.5 Expert Knowledge Elicitation: Interviews with Public Auditors

This section presents the expert knowledge elicitation activities conducted through interviews with public auditors, with the purpose of complementing and critically assessing the findings derived from the systematic literature reviews. While the literature offers valuable insights into analytical methods, data usage, and conceptual approaches, it often abstracts away from the institutional, procedural, and accountability constraints that shape real-world auditing practices. Within the Design Science Research paradigm, engaging with domain experts is therefore essential to ensure that both problem formulation and design decisions are grounded in practice and reflect the needs, expectations, and constraints of the intended users of the proposed artifact.

The interviews were deliberately positioned within the research design as a practice-oriented validation and refinement mechanism and were conducted after the completion of the systematic literature reviews. Rather than aiming to develop a general theory of auditing, their role was to confront the assumptions, limitations, and gaps identified in the literature with practitioners' experiences, particularly with respect to the use of data, risk indicators, and algorithmic support in fraud analysis. By incorporating the perspectives of auditors directly involved in oversight and control activities, this section provides empirical grounding for the framework's design requirements and helps bridge the gap between analytical capabilities and institutional realities, ensuring that the proposed solution is not only theoretically sound but also operationally, legally, and ethically aligned with public-sector auditing practice.

3.5.1 Interview Context and Data Collection

The expert knowledge elicitation involved three public auditors drawn from two key Brazilian oversight institutions: Administrative Council for Economic Defense (CADE) and the Office of the Comptroller General (CGU). Two interviewees were affiliated with CADE, the federal authority responsible for competition policy enforcement and the investigation

of anticompetitive conduct, including collusive practices related to public procurement. The third interviewee was affiliated with the CGU, the federal body responsible for internal control, integrity, and oversight of public administration, with a central role in auditing procurement processes and investigating fraud and corruption within the executive branch. The interviews were conducted as expert knowledge elicitation and focused exclusively on the participants' professional experience and institutional practices related to public procurement oversight. No clinical, health-related, psychological, or other sensitive personal information was collected for analysis, and the procedure involved no experimental intervention or manipulation of participants. Given these characteristics, the interviews were assessed by the researchers as presenting minimal foreseeable risk.

Across both institutions, the interviewed auditors occupy roles directly connected to oversight and investigative activities, combining legal, economic, and analytical perspectives. Their professional experience spans multiple years of engagement with public-sector control functions, including the assessment of procurement procedures, the investigation of collusion and irregularities, and the use of data-driven techniques to support audit and enforcement actions. All interviewees reported regular interaction with structured administrative data, procurement records, and digital information systems, as well as practical exposure to analytical tools and indicators used to prioritize cases and guide investigative efforts. Consistent with the objectives of this study, the description of the interviewees focuses on institutional role, professional experience, and analytical exposure, without reporting personally identifiable information or associating individual responses with identifiable participants. Participation was voluntary, individual responses were treated confidentially, and the findings are reported in a non-identifiable manner. Although prior formal ethical review was not sought for this stage of the research, ethical safeguards were adopted throughout the expert elicitation process, particularly regarding voluntary participation, confidentiality, privacy and protection of participants' identities. These safeguards are consistent with the principles governing research involving human participants under the Brazilian ethical framework ⁴.

3.5.2 Thematic Analysis of Interview Insights

The analysis of the interviews was conducted using a thematic approach, organizing the auditors' insights around recurring patterns that directly relate to the challenges identified in the literature reviews. Rather than attributing statements to individual interviewees,

⁴<https://www.gov.br/conselho-nacional-de-saude/pt-br/camaras-tecnicas-e-comissoes/conep>

the analysis focuses on shared experiences and institutional constraints that characterize fraud investigation practices in public procurement. This thematic organization enables a systematic comparison between academic assumptions and real-world auditing conditions.

A central theme emerging from the interviews concerns the absence of operational decision-support systems tailored to the needs of public auditors. All interviewees emphasized that no dedicated analytical system is currently in place to support fraud risk analysis in procurement, resulting in largely manual, fragmented, and reactive investigative processes. This absence is compounded by the fact that auditors generally do not possess advanced technical training in data analysis, machine learning, or statistics, as their professional backgrounds are predominantly in economics, accounting, law, or related fields. As a consequence, sophisticated analytical outputs—when available—are often difficult to interpret, validate, or operationalize within investigative workflows.

Another prominent theme relates to the limited institutional acceptance of data-driven analysis as evidence. Interviewees consistently reported that purely analytical results, such as anomaly scores or algorithmic outputs, are not considered valid evidence by judicial authorities, nor are they formally accepted as investigative indicators. This constraint significantly restricts the role that analytics can play in enforcement actions and reinforces the need for human judgment, documentary evidence, and legally defensible reasoning throughout the investigative process. As a result, auditors tend to rely on traditional procedural signals and external complaints rather than proactive, data-driven prioritization.

The interviews also revealed substantial challenges associated with data access, fragmentation, and quality. Auditors reported the absence of a unified data repository containing the diverse information required for effective fraud analysis. Relevant datasets are dispersed across multiple systems and institutions, many of which despite being public must be accessed through the same interfaces available to ordinary citizens. Access to more sensitive data, such as fiscal, banking, or telecommunications records, requires formal judicial authorization, introducing significant delays and limiting exploratory analysis. Furthermore, persistent data quality issues, including inconsistent product categorization (e.g., mismatches between NCM codes and actual products) and incompatibilities across datasets, severely constrain data integration and cross-referencing efforts.

Finally, the interviews highlighted structural and institutional constraints affecting investigative capacity. The volume of investigations is low relative to the number of complaints received, largely due to bureaucratic procedures, limited human resources, and

the absence of systematic prioritization mechanisms. Investigations are typically initiated only after formal complaints are submitted and are processed sequentially in a queue. Several auditors noted a preference for investigating smaller cases, as large-scale investigations often involve powerful firms with extensive legal representation, transforming technical inquiries into prolonged political and legal disputes. These conditions collectively reinforce a reactive and risk-averse investigative environment.

3.5.3 Implications for Reference Model Design

The insights derived from the interviews provide direct and actionable implications for the design of the proposed framework. First, the widespread lack of trust in opaque analytical outputs underscores the necessity of embedding explainability as a core design principle. Analytical results must be interpretable and justifiable to auditors who do not possess advanced data science expertise, enabling them to understand, contextualize, and defend analytical findings.

Second, the auditors' explicit concern regarding the risks of automation and judicial non-acceptance of algorithmic evidence reinforces the requirement that the framework be conceived strictly as a decision-support system, rather than as an automated decision-making tool. Human judgment must remain central, with the framework supporting prioritization, exploration, and sense-making rather than replacing institutional authority.

Third, the interviews confirmed the practical relevance of red flags as heuristic risk indicators, while simultaneously exposing their informal and unsystematic use. This finding directly motivates the integration of red flags with AI-based analytics, combining explainable, institutionally familiar indicators with data-driven pattern detection. Such integration allows analytical outputs to be framed as risk signals rather than determinations of wrongdoing.

Fourth, concerns related to responsibility, accountability, and legal defensibility highlight the importance of incorporating data provenance and traceability mechanisms. By explicitly documenting data sources, transformations, and analytical steps, provenance supports auditability and accountability, addressing both institutional and ethical requirements. Finally, the pervasive data quality issues reported by auditors reinforce the need for explicit data validation, transparency, and quality-aware analysis within the framework.

3.5.4 Summary and Link to Artifact Requirements

To make this connection explicit, Table 3.6 synthesizes the evidence derived from the systematic literature reviews and the expert interviews, translating both sources into concrete implications for the design of the proposed reference model. Rather than treating academic and practitioner insights as independent inputs, the table establishes a traceable link between (i) recurring findings in the literature, (ii) institutional constraints and practices reported by public auditors, and (iii) the resulting design needs that inform the framework’s architecture. This synthesis operationalizes the DSR principle of grounding artifact requirements in both rigor and relevance, ensuring that each design decision can be traced back to empirical and theoretical evidence.

Table 3.6: Synthesis of literature and expert interview findings and their implications for model design

Evidence from SLR	Evidence from Expert Interviews	Identified Gap / Design Need	Implication for Design
AI-based fraud detection studies prioritize predictive accuracy, often with limited attention to interpretability or transparency.	Auditors reported low trust in opaque analytical outputs and difficulty understanding or defending algorithmic results.	Lack of explainability undermines institutional trust and practical usability.	Embed explainable analytics and transparent risk indicators as core components.
Many AI approaches implicitly assume automated or semi-automated decision-making.	Algorithmic outputs are not accepted as evidence or formal investigative indicators by judicial authorities.	Automation conflicts with legal and institutional constraints.	Design the system strictly as a decision-support tool, preserving human authority and judgment.
Red flags are discussed in the literature but are rarely integrated in a systematic or formalized manner with AI models.	Auditors rely on informal heuristics and experiential indicators, with no structured prioritization methodology.	Absence of a systematic mechanism to combine heuristics and analytics.	Integrate red flags with AI-based analysis to support explainable risk prioritization.
Several studies rely on proxy labels and weak supervision without addressing data quality implications.	Auditors highlighted pervasive data quality issues, including inconsistent product classification and limited data integration.	Data quality problems compromise both analytical validity and institutional credibility.	Incorporate data quality assessment, transparency, and quality-aware analytics.
Provenance and accountability are discussed in digital government literature but seldom applied to fraud analytics.	Auditors emphasized concerns regarding responsibility, traceability, and decision defensibility.	Lack of traceability limits accountability and legal defensibility.	Implement a provenance layer documenting data sources, transformations, and analytical processes.
Existing approaches rarely consider the technical background of auditors as end users.	Auditors reported limited capacity for advanced data analysis due to their professional training.	Misalignment between system complexity and user capabilities.	Adopt user-centered design and abstractions aligned with auditors’ expertise.
Few studies address investigation prioritization under resource constraints.	Investigations are reactive, complaint-driven, and constrained by limited personnel and bureaucratic processes.	Absence of risk-based prioritization mechanisms.	Support risk ranking and exploratory analysis to guide investigative focus.

Specifically, the table should be read as a mapping mechanism that connects observed gaps and limitations to corresponding design implications. Evidence from the literature highlights methodological tendencies and omissions in existing approaches, while evidence from expert interviews reveals how these approaches align—or fail to align—with real auditing environments. The identified gaps represent points of misalignment between analytical capabilities and institutional realities, which are subsequently addressed through explicit design implications. Together, these elements provide a structured rationale for the architectural components and design principles introduced in the next chapter.

Chapter 4

Methodology, Research Design, and Artifact Development

This chapter presents the methodological foundations, research design, and artifact development process adopted in this thesis. It details how the proposed reference model for fraud risk analysis in PP was conceived, designed, and implemented as a research artifact within a DSR paradigm. The methodology integrates qualitative and technical methods to address a complex socio-technical problem situated at the intersection of digital government, public sector auditing, and data science.

The chapter is structured in three interrelated components. First, it presents the methodological foundations of the study, situating the research within the DSR paradigm and clarifying its epistemological positioning, research cycles, and validation logic. Second, it describes the overall research design, detailing how theoretical knowledge, empirical insights from practitioners, and domain specific constraints were systematically integrated to define problem relevance and design requirements. Third, it explains the artifact development process itself, including requirement elicitation, architectural modeling, implementation decisions, and the incorporation of transparency, accountability, and reproducibility as intrinsic design principles.

4.1 Research Paradigm and Methodological Approach

The research problem addressed in this thesis is inherently socio-technical, as it emerges from the interaction between digital infrastructures, institutional processes, and human decision making within the public sector. Fraud risk analysis in PP does not take place in a purely technical environment, but rather within a complex ecosystem shaped by legal

frameworks, organizational routines, accountability mechanisms, and normative expectations of transparency and fairness. As a result, analytical approaches in this domain must simultaneously engage with technological capabilities and institutional realities.

From a digital government perspective, PP systems are characterized by heterogeneous data sources, evolving regulatory standards, and varying levels of data completeness and quality. These characteristics introduce structural constraints that limit the applicability of purely data driven solutions and challenge assumptions commonly made in predictive or classification oriented AI research. Moreover, auditing practices rely not only on analytical outputs, but also on interpretability, traceability, and the possibility of contesting results, since investigative and enforcement actions remain subject to legal scrutiny and institutional responsibility.

Consequently, fraud risk analysis in PP cannot be framed solely as a ML or optimization problem. Instead, it must be understood as a sociotechnical problem in which analytical systems operate as decision support mechanisms embedded in broader governance structures. This perspective implies that system design choices, such as the level of automation, the form of analytical outputs, and the mechanisms for explanation and accountability, are as critical as algorithmic performance. Recognizing the sociotechnical nature of the problem is therefore a foundational assumption of this research and directly motivates the adoption of a methodological approach that integrates technical design with institutional and human considerations.

This research is characterized as applied, problem driven, and artifact oriented, reflecting both its motivation and its mode of knowledge production. Rather than pursuing purely theoretical explanations or methodological novelty in isolation, the study is grounded in a concrete public sector problem and seeks to generate actionable knowledge through the design and evaluation of a computational artifact.

From an applied research perspective, the work is motivated by practical challenges faced by public oversight and auditing institutions in analyzing fraud risk within large scale PP ecosystems. The intended contribution extends beyond descriptive insights, aiming to support real world decision making by providing a structured reference model capable of operating under the constraints of public administration, such as transparency and accountability. As such, relevance to practice is treated as a core research objective.

The study is also problem-driven, as its research questions and design choices originate from observed limitations in existing approaches to fraud detection in PP. These limitations include the reliance on weak or proxy labels, insufficient attention to institutional

constraints, and limited integration between analytical techniques and audit practices. Consequently, the research does not begin with data availability or algorithm selection, but with a careful examination of the problem context and its associated requirements.

Finally, the research is artifact oriented, with the primary outcome being a reference model designed to support fraud risk analysis. In this context, knowledge contributions are embedded in the artifact itself specifically in its architectural structure, design principles, and operational mechanisms, rather than solely in empirical findings or theoretical propositions. The artifact functions as the central vehicle through which analytical, institutional, and ethical considerations are integrated and made explicit, aligning the research with a constructive and prescriptive mode of inquiry.

4.2 Design Science Research Framework

This section presents the DSR framework adopted in this thesis and explains how it structures the overall research process. The objective is to formally introduce the DSR model that guides the study, clarify its core stages, and justify its suitability for addressing the research problem at hand. In addition, this section delineates how the different phases of the adopted DSR model are mapped to the organization of the thesis, providing a coherent methodological backbone that links problem identification, artifact design and development, instantiation, and evaluation within a unified research framework.

4.2.1 DSR strategy

This thesis adopts the DSR framework proposed by Hevner et al. (HEVNER, 2007) as the guiding methodological model. The choice of this model is grounded in its strong theoretical foundation within IS research and its explicit focus on the rigorous design and evaluation of artifacts intended to address real-world problems. Hevner's DSR framework conceptualizes research as an iterative process that balances relevance to practice and rigor in knowledge production, making it particularly suitable for sociotechnical domains such as digital government and public sector auditing.

The adoption of Hevner's model is further justified by its clear articulation of the relationships between the problem environment, the knowledge base, and the designed artifact. In the context of this thesis, fraud risk analysis in public procurement is shaped by institutional constraints, accountability requirements, and heterogeneous data infrastructures. Hevner's framework explicitly acknowledges such contextual factors by posi-

tioning the artifact as a mediating construct between organizational needs and scientific knowledge, thereby supporting the development of solutions that are both theoretically grounded and operationally viable. This thesis adopts the DSR framework proposed by Hevner et al. (HEVNER, 2007) as the guiding methodological model. The choice of this model is grounded in its strong theoretical foundation within IS research and its explicit focus on the rigorous design and evaluation of artifacts intended to address real-world problems. Hevner’s DSR framework conceptualizes research as an iterative process that balances relevance to practice and rigor in knowledge production, making it particularly suitable for sociotechnical domains such as digital government and public sector auditing.

Figure 4.1 illustrates how the DSR paradigm is operationalized throughout this thesis. The framework is organized around three complementary components: the application domain, the knowledge foundations, and the central build–evaluate design cycle. Together, these components demonstrate how practical problems and theoretical knowledge are integrated to support the development and evaluation of the proposed reference model. On the left, the application domain situates the research within the context of public procurement oversight, identifying the main stakeholders, organizational and technical environments, and the practical challenges that motivate the study, including fraud and collusion, fragmented data ecosystems, limited traceability, and the need for data-driven oversight. These contextual elements drive problem identification, the elicitation of practical requirements, and the systematic literature reviews that establish the relevance of the research.

On the right, the foundations represent the knowledge base supporting artifact development. They combine kernel theories, including data provenance, Open Government Data, trustworthy AI, risk-based auditing, and sociotechnical systems, with domain expertise from public procurement and audit practice, as well as existing meta-artifacts such as fraud detection models and red flag methodologies. At the center, the design cycle iteratively develops and evaluates the proposed reference model. The development phase integrates the analytical framework with ethical principles, governance and security mechanisms, and evaluation and refinement processes into a unified reference model. The evaluation phase operationalizes the artifact through empirical instantiation and assesses it by means of institutional validation, institutional adequacy assessment, and comparative analysis. This iterative process ensures that the resulting artifact remains simultaneously relevant to real-world auditing practice and rigorously grounded in established scientific knowledge.

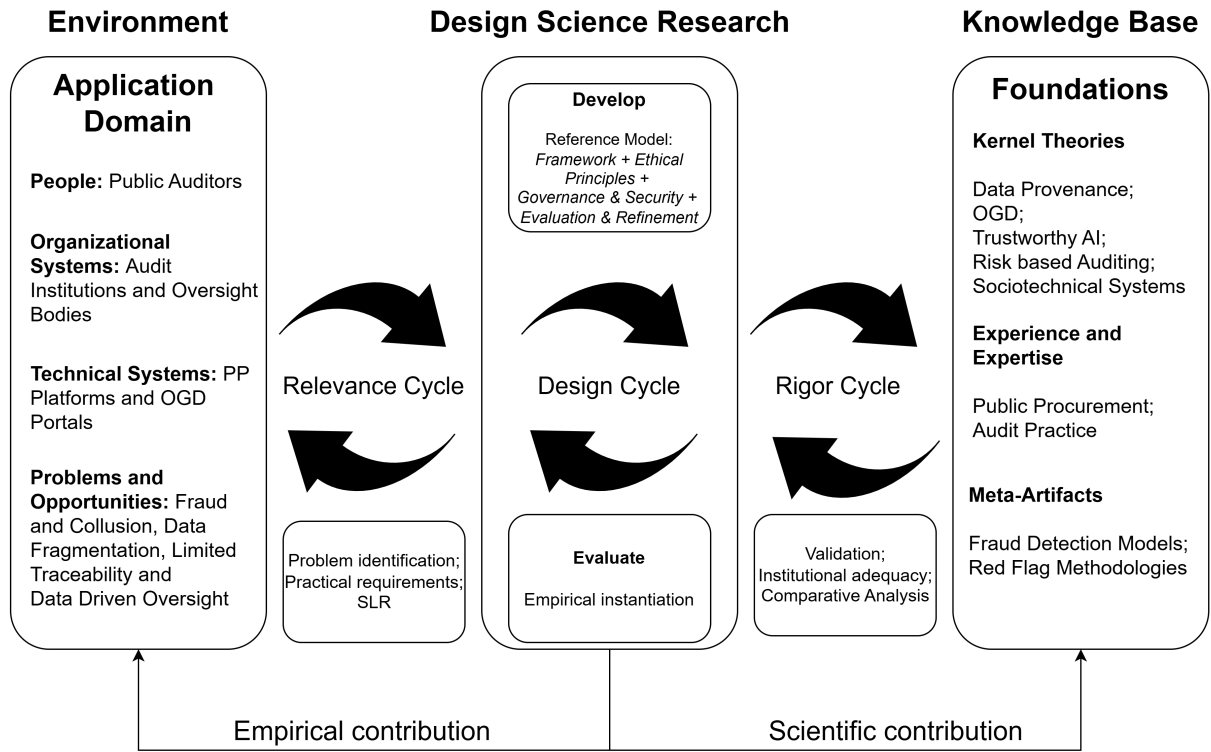


Figure 4.1: Research Framework. Based on (BHAROSA, 2011)

By adopting Hevner’s DSR model, this thesis situates the development of the proposed framework within a well-established methodological structure that supports iterative refinement, methodological rigor, and practical relevance. The following subsection maps these DSR stages to the specific chapters and methods employed throughout the thesis, making explicit how the adopted framework structures the overall research design.

4.2.2 Mapping DSR Stages

The DSR process adopted in this thesis is structured around the interaction between the application domain, the foundational knowledge base, and the central design cycle responsible for artifact development and evaluation. Rather than treating DSR stages as strictly linear steps, the research operationalizes them as interconnected components that continuously inform and refine one another.

The process begins with a structured engagement with the application domain, which defines the research motivation and contextual constraints. This domain comprises public auditors, audit institutions, PP platforms, and OGD systems, as well as persistent challenges such as fraud risk, data fragmentation, and limited traceability. Problem identification emerged from the articulation of these contextual challenges and was supported

by SLR and interviews with public auditors.

In parallel, the research is anchored in the foundational knowledge base, which provides theoretical grounding and scientific rigor. Kernel theories such as data provenance, OGD, trustworthy AI, risk based auditing, and sociotechnical systems inform the conceptual structure of the artifact. Additionally, domain specific experience in PP and audit practice contributes contextual expertise, while prior meta-artifacts, including fraud detection models and red flag methodologies, serve as design references.

At the core of the research lies the design cycle, which operationalizes the development and evaluation of the proposed reference model. The development phase encompasses the reference model design, including the framework (data, engine, and decision layers), as well as the integration of ethical principles, governance and security mechanisms, and evaluation and refinement components.

The evaluation component of the design cycle assesses the artifact through empirical instantiation and institutional validation. Demonstration is achieved by applying the reference model to distinct public procurement contexts, including Brazil and the Netherlands, illustrating its adaptability across heterogeneous institutional environments. Evaluation activities include empirical analysis of generated risk signals, assessment of interpretability and traceability, institutional adequacy analysis, expert validation with auditors, and comparative analysis across contexts.

Finally, communication is embedded throughout the research lifecycle. Intermediate findings and conceptual developments have been disseminated through peer-reviewed publications, conference presentations, and academic discussions, contributing to cumulative knowledge in digital government, public procurement, and DSR. The thesis consolidates these contributions into a coherent reference model positioned at the intersection of technical rigor and institutional legitimacy.

Table 4.1 synthesizes the mapping between the core components of the adopted DSR structure, the corresponding research purposes, the methods employed, and the chapters of the thesis in which each component is operationalized. Rather than presenting DSR as a strictly linear sequence of stages, the table reflects its structured configuration around the application domain (relevance), the foundational knowledge base (rigor), and the iterative design cycle responsible for artifact development and evaluation. By explicitly linking contextual grounding, theoretical foundations, artifact construction, and empirical assessment to concrete methodological activities, the table ensures transparency and methodological coherence. It provides a consolidated overview of how practical problem

identification, theoretical grounding, reference model design, empirical instantiation, and institutional validation are systematically integrated throughout the research process.

Table 4.1: Mapping of DSR stages to research methods and thesis chapters

DSR Components	Purpose	Methods	Thesis Chapter
Application Domain (Relevance)	Understand contextual constraints and define the research problem	SLR; Interviews with Public Auditors; Problem Identification; Definition of Practical Requirements	Literature Reviews; Expert Knowledge Elicitation
Foundations (Rigor)	Ground the artifact in theoretical and domain knowledge	Synthesis of Kernel Theories; Analysis of Meta-Artifacts; Conceptual Modeling	Theoretical Foundations; Methodology
Design Cycle (Develop)	Construct the reference model artifact	Reference Model Design	Artifact Design and Development
Design Cycle (Evaluate)	Assess artifact utility, robustness, and institutional adequacy	Empirical Instantiation; Signal Analysis; Expert Validation; Institutional Adequacy Assessment; Comparative Analysis	Reference Model Instantiation; Results and Validation

4.3 Artifact Design and Development

This section describes the design and development of the research artifact proposed in this thesis, namely reference model for fraud risk analysis in PP grounded in OGD. Following the DSR paradigm, the artifact is conceived as a purposeful and actionable construct designed to address a concrete sociotechnical problem faced by public sector auditing and oversight institutions. The development of the artifact is informed by the design requirements elicited from the SLR and expert interviews discussed in earlier chapters. These requirements reflect not only functional concerns, such as data integration, indicator computation, and analytical scalability, but also non functional considerations related to transparency, traceability, reproducibility, and ethical accountability. Accordingly, the artifact is designed as a modular and extensible reference model, in which analytical components are explicitly connected to governance mechanisms that support responsible use in public-sector contexts.

4.3.1 Design Requirements

The design requirements that guided the development of the proposed artifact were elicited from two complementary sources: SLR and empirical insights obtained from public auditors. At this stage, the focus is not on reporting the full review protocols or interview procedures, but on synthesizing the resulting requirements that informed the artifact de-

sign. The detailed description of the literature reviews and auditor interviews is presented in the Chapter 3.

Evidence synthesized from the SLR reveals recurring structural limitations in existing approaches to fraud detection and risk analysis in PP, particularly regarding the use of labeled data. A predominant pattern in the literature is the reliance on supervised or semi-supervised ML techniques trained on proxy or weak labels, such as ex post sanctions, media exposure, judicial outcomes, or heuristic assumptions. Although these sources provide partial signals of irregularity, they do not necessarily represent verified or exhaustive instances of fraud. Moreover, the number of officially confirmed fraud cases is typically negligible when compared to the total volume of procurement transactions, resulting in extreme class imbalance and rendering fully supervised learning approaches methodologically fragile. This structural constraint does not preclude the use of AI, but it demands careful methodological design. Under conditions of limited and imperfect labeling, fraud risk analysis must move beyond exclusive dependence on ground truth datasets and instead combine weak supervision strategies, heuristic based labeling functions, domain informed rules, and unsupervised learning techniques capable of detecting anomalous or outlier patterns without predefined labels. These approaches may be further complemented by more conventional analytical risk indicators derived from structured statistical analysis. Consequently, a central design requirement emerging from the literature is that the proposed artifact must operate robustly in low label environments, integrating AI based techniques with transparent, rule explicit, and data driven indicators that enhance interpretability, analytical resilience, and institutional legitimacy.

Another limitation consistently observed in the reviewed studies concerns the limited attention given to interpretability and accountability. While many approaches report predictive performance metrics, they frequently provide insufficient explanations of how risk signals are generated or how analytical outputs relate to underlying procurement data. In the context of public sector auditing, such opacity undermines the usability of analytical tools, as results must be explainable, contestable, and defensible under legal and institutional scrutiny. This led to the requirement that all indicators and analytical components within the artifact must be explicitly defined in terms of their calculation logic, input data, and assumptions, enabling auditors to understand and justify the produced risk signals.

Empirical insights obtained from interviews with public sector auditors highlighted challenges related to data heterogeneity and fragmentation across public procurement

ecosystems. Auditors consistently emphasized that fraud risk analysis in practice requires combining information from multiple procurement platforms, registries, and auxiliary government datasets, each characterized by distinct schemas, update cycles, and quality levels. According to these practitioners, analytical approaches based on isolated datasets or narrowly scoped procurement systems are insufficient to capture complex risk patterns that span multiple procedures, suppliers, or institutional contexts. In addition, auditors stressed the importance of maintaining clear documentation of how data are integrated and transformed, particularly in contexts subject to legal scrutiny and accountability requirements. These observations led to the requirement that the artifact should be designed to operate over integrated and heterogeneous data sources, while incorporating explicit provenance and traceability mechanisms that document how analytical outputs are derived from raw data.

Another important finding from the interviews concerns the role of AI-supported fraud risk analysis within public auditing. Auditors consistently emphasized that such systems should function as decision support tools rather than fully automated decision-making systems. Analytical outputs are primarily used to support prioritization, exploratory analysis, and case selection, while investigative decisions remain the responsibility of human professionals operating under legal and institutional accountability. According to these practitioners, automation without appropriate mechanisms for interpretation and contestation would be incompatible with established auditing workflows and governance requirements. Consequently, the proposed artifact must explicitly preserve human judgment as a central component of the auditing process, providing structured risk signals without replacing expert decision-making. Together with the other practice-derived requirements, this reinforces the need for a reference model that balances analytical capability with transparency, accountability, and institutional trust.

Table 4.2 summarizes the consolidated set of functional and non-functional design requirements that guided the development of the proposed artifact. The functional requirements define the core capabilities expected from the artifact, such as label independent risk analysis, red flag based assessment, integration of heterogeneous data sources, and decision-support orientation. The non-functional requirements capture cross cutting properties related to interpretability, provenance, transparency, accountability, and extensibility, which are essential for the responsible deployment of analytical systems in PP. Together, these requirements establish a structured design baseline that informs subsequent architectural and implementation decisions presented in the following sections.

Table 4.2: Functional and Non-Functional Design Requirements

ID	Type	Description	Source
R1	Functional	The artifact shall support fraud risk analysis under conditions of limited and imperfect labeling, combining weak supervision strategies, heuristic based labeling functions, unsupervised learning techniques, and transparent rule explicit indicators rather than relying exclusively on fully supervised classification models.	SLR
R2	Functional	The artifact shall implement a red flag based analytical engine capable of generating structured risk signals to support exploratory analysis, prioritization, and case selection in PP.	SLR
R3	Functional	The artifact shall operate over integrated and heterogeneous data sources, including procurement records and auxiliary government datasets, in order to support cross contextual and relational risk analysis.	Auditor Interviews
R4	Functional	The artifact shall function as a decision support system, providing analytical outputs that assist auditors while explicitly preserving human judgment and investigative authority.	Auditor Interviews
R5	Non-functional	All risk indicators and analytical rules shall be formally specified and documented, including their conceptual rationale, calculation formula, parameters, and decision thresholds, ensuring semantic clarity and methodological consistency.	SLR
R6	Non-functional	The artifact shall implement operational provenance mechanisms record data lineage, transformations, model executions, and parameter configurations associated with each generated risk signal, ensuring technical traceability and reproducibility	Auditor Interviews
R7	Non-functional	The artifact shall enable institutional transparency and accountability by providing mechanisms for structured inspection, explanation, and justification of analytical outputs in contexts of organizational oversight and legal scrutiny.	SLR and Auditor Interviews
R8	Non-functional	The artifact shall be modular and extensible, allowing the addition, modification, or removal of indicators and data sources without compromising the overall framework structure or governance principles.	SLR

4.3.2 The Reference Model

This thesis proposes a reference model for fraud risk analysis in PP that structures the transformation of heterogeneous and OGD into formally defined and analytically grounded risk indicators. Rather than constituting a standalone predictive model, the artifact is conceived as a layered sociotechnical model that integrates data integration mechanisms, a structured risk analytics engine, and a decision support layer that organizes, contextualizes, and prioritizes risk signals for human evaluation. Crucially, the reference model extends beyond a purely technical framework by explicitly incorporating ethical principles,

governance and security mechanisms, and structured evaluation and refinement processes as integral architectural layers.

Figure 4.2 presents the proposed reference model. The core of the artifact, highlighted in blue, is vertically structured around three primary layers: *Data*, *Engine*, and *Decision*, representing the logical and analytical flow of fraud risk analysis in PP. Complementing this structure, the reference model also incorporates transversal dimensions that span all layers of the model. More specifically, the elements highlighted in gray and orange represent ethical constraints and requirements that regulate and shape the operation of the model, while the elements highlighted in green represent enabling structural capabilities responsible for sustaining, governing, evaluating, and continuously refining the operational lifecycle of the artifact.

The *Data Layer* is responsible for the ingestion, integration, and harmonization of heterogeneous and open datasets. It includes structured data acquisition pipelines, meta-data preservation mechanisms, schema alignment procedures, and embedded data quality controls. This layer establishes the informational foundation upon which risk indicators are constructed, ensuring that data transformations are systematic, reproducible, and semantically coherent.

The *Engine Layer* operationalizes fraud-related domain knowledge. It integrates heuristic red-flag logic with analytical and AI-based techniques for risk characterization, anomaly detection, and prioritization. By combining rule based, data driven mechanisms, and AI methods this layer transforms harmonized data into analytically grounded risk assessments while preserving interpretability and traceability.

The *Decision Layer* translates analytical outputs into actionable decision-support artifacts for auditors and oversight bodies. It provides functionalities such as risk triage, case prioritization, structured evidence exploration, explainability interfaces, and workflow support for reporting and investigation management. This layer bridges analytical computation and institutional action.

Surrounding the core, the model explicitly incorporates a set of ethical principles (highlighted in gray): *Human Oversight*, *Transparency and Explainability* and *Accountability*. These elements are not implemented as independent functional modules but operate as systemic constraints that shape the design and operation of all three core layers. They define the ethical and boundaries within which data processing, risk modeling, and decision support must occur.

In addition to these ethical principles, the reference model also incorporates *Provenance* (highlighted in orange) as a transversal requirement that spans the entire model. Unlike the ethical principles previously discussed, provenance is not treated as a normative constraint itself, but rather as a foundational mechanism responsible for sustaining traceability, reproducibility, auditability, and analytical transparency across all operational layers. In practical terms, provenance enables every red flag, analytical result, and decision-support artifact generated by the framework to be systematically linked back to its originating data sources, transformation procedures, analytical logic, intermediate artifacts, and responsible actors.

Complementing these constraints, two enabling structural capabilities (highlighted in green) span the entire architecture: *Evaluation and Refinement* and *Governance and Security*. These components represent what must be continuously performed to sustain the reference model in practice. *Evaluation and Refinement* ensures iterative validation of red flags, analytical performance, institutional adequacy, and alignment with auditing practices. It operationalizes feedback loops from auditors and domain experts, enabling the systematic evolution of indicators and analytical mechanisms. *Governance and Security* establishes the organizational and technical safeguards necessary for responsible operation, including access control, role definition, compliance mechanisms, data protection policies, and monitoring of system usage.

The arrows connecting the *Data*, *Engine*, and *Decision* layers represent the logical and informational flow of the reference model, which originates in the Data Layer and progressively increases in semantic abstraction. Harmonized and quality-controlled data are consumed by the Engine Layer to compute red flags and characterize fraud risk patterns. These analytical outputs are then transformed into structured decision-support artifacts within the Decision Layer, enabling prioritization and investigative action.

By explicitly distinguishing between (i) the operational core of the system, (ii) normative constraints that regulate its functioning, and (iii) structural capabilities that ensure its sustainability and institutional robustness, the architecture positions the reference model as a layered sociotechnical blueprint. Rather than constituting a standalone predictive system, the artifact defines a structured and governable decision-support environment in which fraud risk analysis is analytically grounded, ethically constrained, and institutionally accountable.

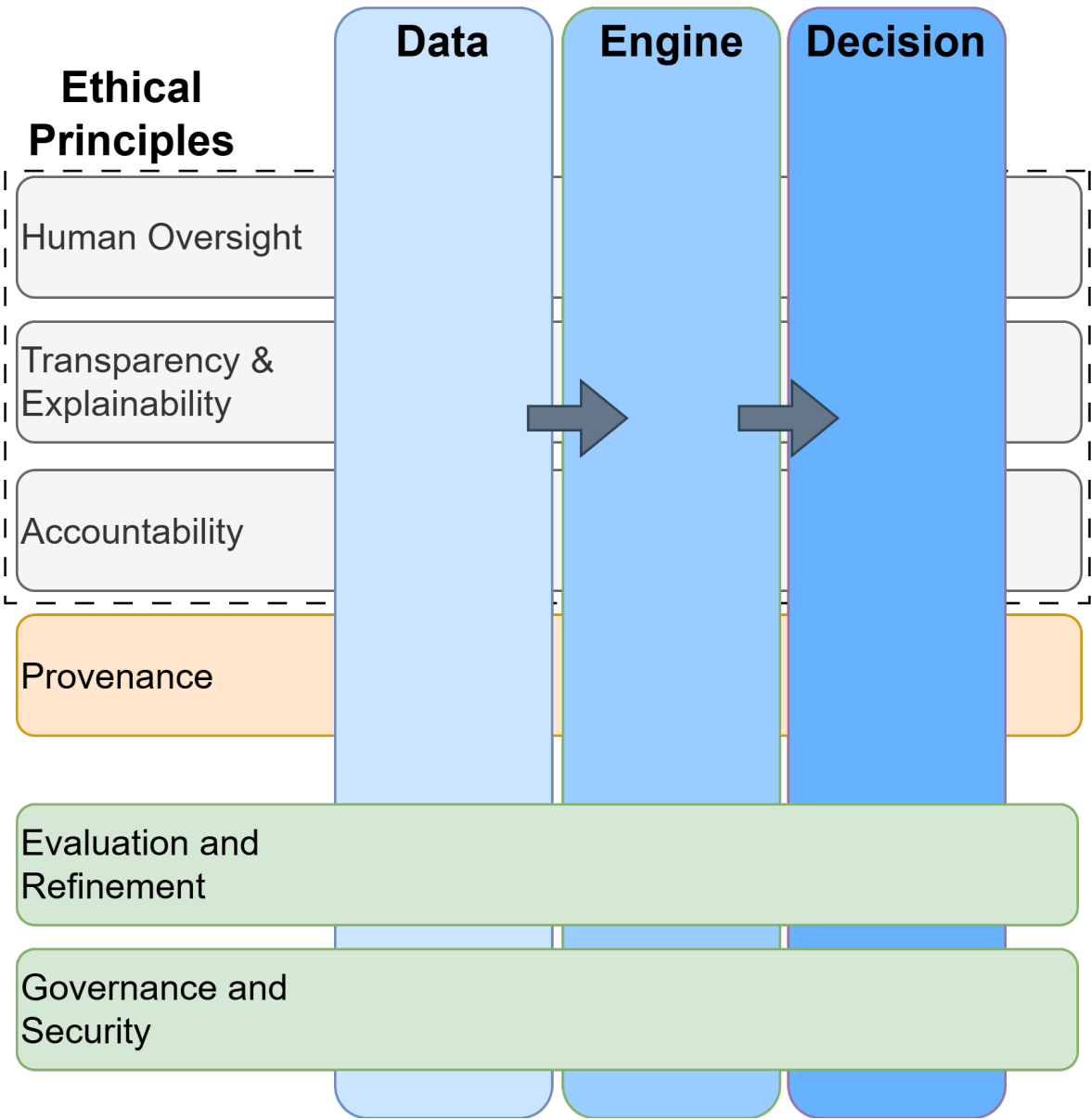


Figure 4.2: Reference Model

4.3.3 Data Layer

The Data Layer constitutes the foundational layer of the proposed reference model, as the reliability of fraud risk indicators and subsequent audit oriented assessments is intrinsically dependent on the quality, completeness, and interoperability of the underlying data. In the context of PP, OGD are typically distributed across heterogeneous portals and institutional repositories, varying substantially in structure, granularity, update frequency, and semantic consistency. Accordingly, this layer is responsible for establishing a controlled and reproducible data pipeline that collects procurement and auxiliary datasets, preserves acquisition metadata, and transforms raw records into a harmonized

analytical representation suitable for downstream risk analysis. By ensuring that heterogeneous sources are systematically curated and validated before they reach the analytical components of the framework, the Data Layer reduces noise and integration artifacts, supports traceable evidence extraction, and provides a stable basis for the Engine Layer to compute red flags and characterize fraud related risk patterns.

To operationalize these objectives, the Data Layer is conceptually structured into three interdependent components: *Data Sources and Registration*, *Acquisition*, and *Data Lakehouse*. The *Data Sources* component is responsible for systematically identifying, registering, and cataloging all relevant institutional data domains that may contribute to fraud risk analysis. This includes core procurement databases, broader government administrative datasets, and complementary contextual data sources. Its primary responsibility is to establish a controlled and documented inventory of inputs, clarifying institutional provenance, scope, and analytical relevance of each dataset incorporated into the reference model.

The *Acquisition* component governs the operational retrieval of registered data sources. It encompasses API extraction routines, bulk download mechanisms, controlled parameter definition for queries, and structured metadata management associated with each ingestion event. Its responsibility is to ensure that data collection is reproducible, traceable, and technically controlled, preserving information about extraction logic, versioning conditions, and access endpoints. The *Data Lakehouse* component provides the structured environment for data consolidation, transformation, modeling, and catalog management. It integrates transformation rules, schema alignment, identifier reconciliation, and database modeling activities into a unified architectural layer. Its responsibility is to convert heterogeneous raw inputs into harmonized and semantically coherent datasets that are analytically ready, quality controlled, and properly documented for downstream consumption.

Figure 4.3 illustrates how these components interact in a structured flow that transforms raw institutional data into refined analytical assets. The process begins with institutional repositories, procurement databases, government data, and additional contextual sources, which serve as inputs to the *Data Sources* component. Sources are then operationally ingested through the *Acquisition* component, where extraction routines and parameters define controlled data retrieval and produce structured raw datasets accompanied by metadata. These datasets are subsequently processed within the *Data Lakehouse*, where transformation, cataloging, and database modeling activities generate harmonized

and refined data. The output of the Data Layer is therefore a modeled datasets, which serves as the formal input to the Engine Layer, enabling structured red flag computation and risk analytics while maintaining traceability and institutional coherence.

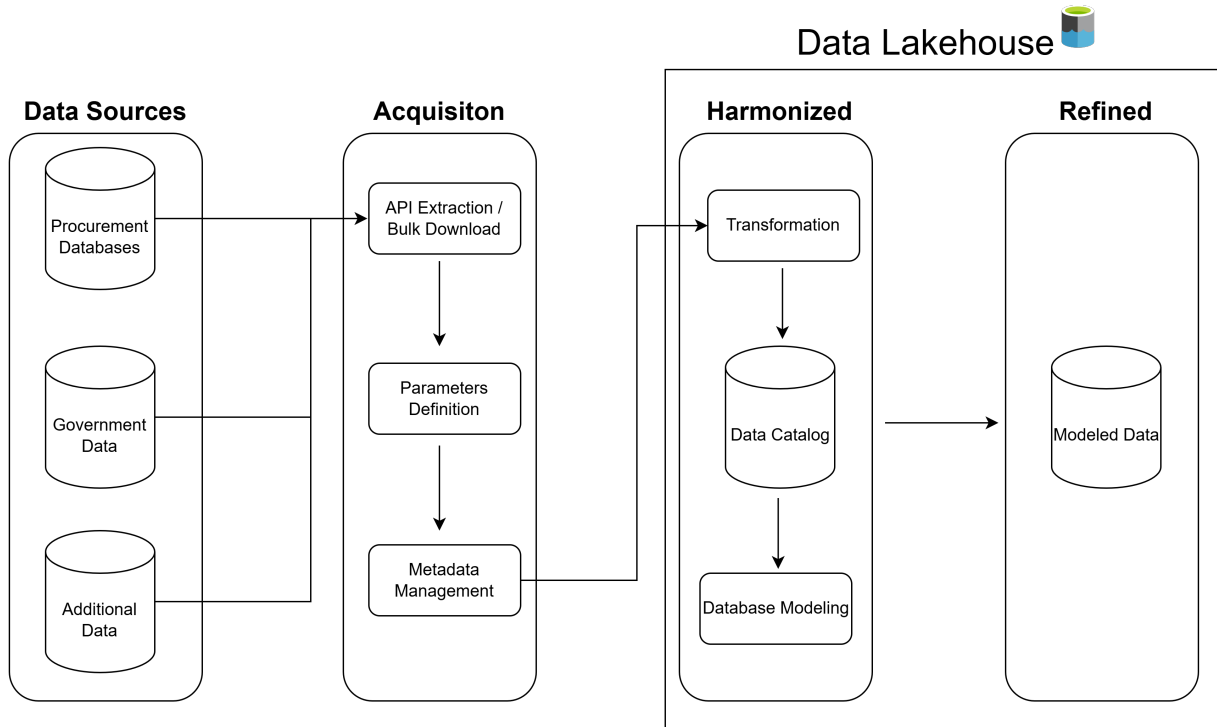


Figure 4.3: Data Layer

4.3.4 Engine Layer

The Engine Layer represents the analytical core of the proposed framework, where refined procurement data are transformed into fraud risk signals that can effectively support auditing activities. While the Data Layer ensures that heterogeneous OGD are curated into a stable and interoperable analytical schema, the Engine Layer operationalizes fraud related knowledge by computing red flags, characterizing suspicious patterns, and producing interpretable risk assessments. Conceptually, this layer receives as input the unified procurement entities and contextual information generated in the Data Layer (e.g., contracts, suppliers, contracting authorities, items, amendments, and auxiliary registries) and produces as output a structured set of risk indicators, aggregated risk scores, and prioritization artifacts. Importantly, the Engine Layer is designed to remain functional under the practical constraints of the public sector by combining deterministic indicators with analytical and learning-based mechanisms. As a result, the Engine Layer bridges raw evidence and auditor centered decision support, ensuring that downstream prioritization is not merely predictive, but evidence grounded and amenable to scrutiny.

To operationalize these objectives, the Engine Layer is decomposed into three complementary components: *Heuristic*, *Analytical*, and *AI*. First, the *Heuristic* component implements rule based red flags grounded in domain knowledge and audit practice, translating well established suspicious patterns into deterministic indicators with explicit thresholds and evidence pointers. This component ensures baseline transparency and supports direct interpretability, allowing auditors to understand why a case is flagged and to trace each signal back to the triggering procurement records. Second, the *Analytical* component provides statistical and pattern oriented mechanisms to contextualize procurement behavior and detect irregularities that may not be fully captured by deterministic rules, such as distributional anomalies, supplier concentration patterns, temporal outliers, and abnormal relationships between prices, quantities, and procurement modalities. Third, the *AI* component incorporates learning based techniques to synthesize indicator information and enhance prioritization performance when feasible, including unsupervised clustering, weak supervision pipelines, or supervised models trained on proxy labels and expert feedback.

The Figure 4.4 illustrates the conceptual flow of the Engine Layer, highlighting how different forms of analytical reasoning are articulated to transform refined data into structured and interpretable risk artifacts. This layer receives as input the procurement entities already integrated and validated by the Data Layer and operates as the analytical core of the reference model, in which risk signals are identified, contextualized, and organized without producing automated decisions. The design explicitly shows a deliberate separation between three analytical components, *Heuristics*, *Analytical*, and *AI*, that reflect distinct sources of knowledge about risk and operate in a complementary way throughout the pipeline. It is important to emphasize, however, that the specific analytical mechanisms represented within each of these sublayers correspond to illustrative design options rather than mandatory components. The boxes depicted under the Heuristics, Analytical, and AI sublayers represent suggested or potential analytical strategies that may be adopted depending on institutional context, data availability, and analytical maturity. Not all mechanisms need to be implemented simultaneously; rather, the architecture defines a structured space of possibilities within which different combinations of rule-based logic, statistical analysis, and AI driven modeling can be selectively operationalized.

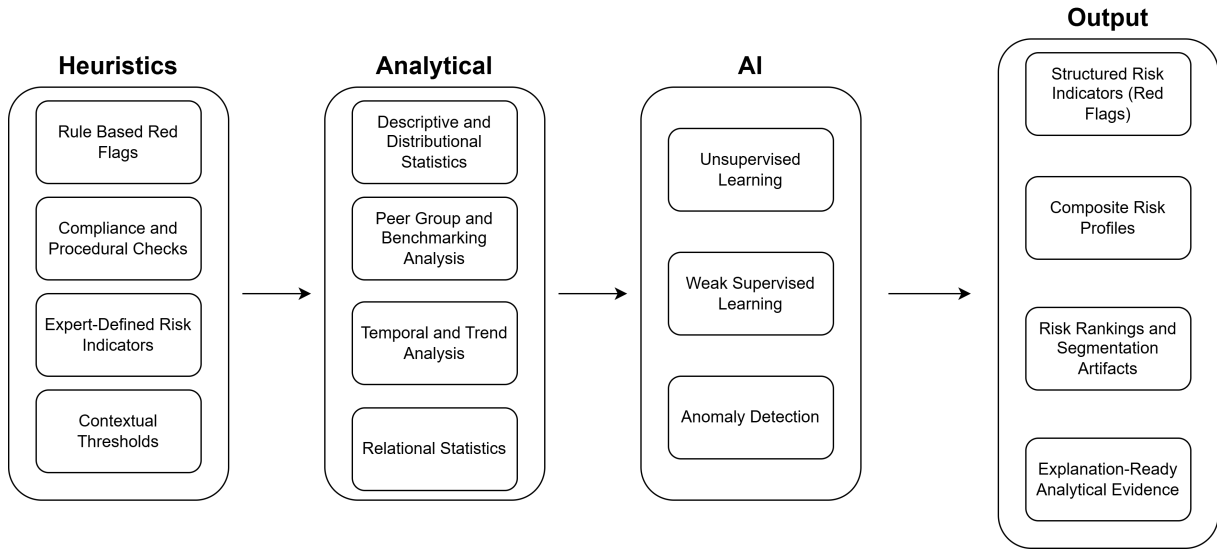


Figure 4.4: Engine Layer

The Heuristics component formalizes explicit, rule-driven knowledge about fraud and irregularities in PP, translating normative, procedural, and experiential insights into deterministic risk indicators. This component is grounded in logical predicates, threshold based conditions, and boolean or ordinal decision rules derived from legislation, audit manuals, and expert practice. Typical mechanisms include rule based red flags, which activate when predefined conditions are met (e.g., low competition, repeated winners, excessive contract amendments), compliance and procedural checks that verify adherence to mandatory process constraints (such as legal deadlines or procurement modalities), and expert defined risk indicators reflecting recurrent suspicious patterns observed by auditors but not necessarily codified in law. To mitigate rigidity and reduce false positives, contextual thresholds are employed, allowing rule parameters to vary according to sectoral, temporal, or market-specific baselines. Mathematically, these mechanisms rely on deterministic functions, conditional logic, and simple aggregations, ensuring that each activated signal is directly interpretable and traceable to its triggering condition. As a result, the heuristics component establishes a transparent and auditable baseline for risk detection, independent of statistical inference or learning based adaptation.

The Analytical component relies exclusively on classical statistical techniques to identify irregularities through quantitative comparison, without employing any form of machine learning or data-driven model training. Its purpose is to contextualize procurement behavior by detecting deviations from expected statistical patterns within peer groups, time periods, or relational structures. Core mechanisms include descriptive and distributional statistics, such as measures of central tendency, dispersion, quantiles, and outlier

detection based on interquartile ranges or standardized scores, used to identify extreme or atypical values (e.g., abnormal prices or contract volumes). Peer group and benchmarking analysis compares entities against statistically similar counterparts, enabling relative assessments normalized by sector, size, or modality. Temporal and trend analysis examines changes over time, identifying abrupt shifts, growth patterns, or recurrent anomalies using moving averages, rate-of-change measures, or simple trend decompositions. Finally, relational statistics capture structural properties of procurement interactions through non-learning network measures, such as frequency of co-occurrence, degree distributions, or concentration ratios. By relying on well-established statistical principles, this component provides stable, explainable, and reproducible evidence of anomalous behavior that complements deterministic heuristics without introducing algorithmic opacity.

The AI component introduces learning based techniques in a constrained and purpose specific manner, focusing on pattern discovery, signal synthesis, and anomaly scoring rather than automated decision making. Unsupervised learning methods, such as clustering or density based techniques, are employed to uncover latent structures in procurement data, grouping entities with similar behavioral profiles and highlighting atypical clusters without requiring labeled fraud cases. Anomaly detection techniques assign continuous anomaly scores based on multivariate deviations from learned normal behavior, supporting prioritization by degree of abnormality rather than binary classification. Weak supervised learning addresses the scarcity of verified fraud labels by leveraging imperfect supervision sources, such as heuristic indicators or expert annotations, as probabilistic or noisy labels, enabling models to infer latent risk patterns under uncertainty. Conceptually, these methods rely on optimization objectives, distance metrics, likelihood estimation, or probabilistic aggregation of weak signals. Crucially, the AI component is designed to synthesize and amplify signals generated by heuristic and statistical analyses, while remaining subordinate to them in terms of interpretability and governance. Learning based outputs are therefore treated as advisory signals whose use is conditional, contextual, and subject to human oversight.

The combined operation of the Heuristics, Analytical, and AI components culminates in a set of structured analytical artifacts that form the formal output of the Engine Layer and the input to the Decision Layer. These artifacts include structured risk indicators (Red Flags), which encode individual signals of potential irregularity along with their activation logic and supporting evidence; Composite Risk Profiles, which aggregate multiple indicators into coherent representations of risk at the level of contracts, suppliers, or processes; and Risk Rankings and Segmentation Artifacts, which express relative

risk through ordered lists or behavioral groupings rather than absolute judgments. Additionally, explanation ready analytical evidence packages the underlying calculations, statistical summaries, and data references required to justify each risk characterization. Collectively, these outputs do not represent decisions or determinations of fraud, but rather interpretable, evidence anchored representations of risk that enable prioritization, exploration, and professional judgment. By explicitly materializing these artifacts, the framework enforces a clear separation between analytical reasoning and institutional decision making, ensuring that downstream actions remain human controlled, auditable, and accountable.

4.3.5 Decision Layer

The Decision Layer represents the interaction and action oriented layer of the reference model, where analytical outputs generated by the Engine Layer are transformed into auditor centered decision support capabilities. While the Engine Layer focuses on computing fraud related risk indicators and assessments, the Decision Layer is responsible for structuring, contextualizing, and presenting these outputs in a form that aligns with professional auditing workflows and institutional decision making processes. Conceptually, this layer consumes structured risk knowledge, interpretable risk assessments, and evidence anchored analytical artifacts produced by the Engine Layer, and delivers decision support functionalities that enable risk triage, exploratory analysis, and prioritization of audit efforts. The Decision Layer is explicitly designed to preserve human oversight and professional judgment, ensuring that auditors remain responsible for interpreting analytical results, validating evidence, and determining appropriate investigative or administrative responses.

To operationalize these objectives, the Decision Layer is decomposed into three interrelated components: *Risk Prioritization*, *Evidence Exploration and Explainability*, and *Workflow and Reporting Support*. The *Risk Prioritization* component structures analytical outputs to support comparative assessment across procurement entities, contracts, or suppliers, enabling auditors to identify cases with elevated risk profiles and allocate limited investigative resources more effectively. The *Evidence Exploration and Explainability* component provides mechanisms for inspecting the analytical rationale underlying each risk assessment, including drill down capabilities, indicator level explanations, and traceable links to the underlying data and transformations. This component ensures that risk signals can be scrutinized, contested, and understood in institutional and legal contexts.

Finally, the *Workflow and Reporting Support* component aligns analytical insights with auditing and oversight processes, supporting documentation, case handling, and reporting activities.

Figure 4.5 depicts the workflow of the Decision Layer, which structures how analytically generated risk signals are transformed into decision support outcomes that are suitable for public sector auditing contexts. This layer does not aim to automate investigative or enforcement decisions. Instead, it mediates between upstream analytical outputs and downstream human judgment by introducing explicit procedural gates that separate analytical relevance, evidentiary availability, and institutional use.

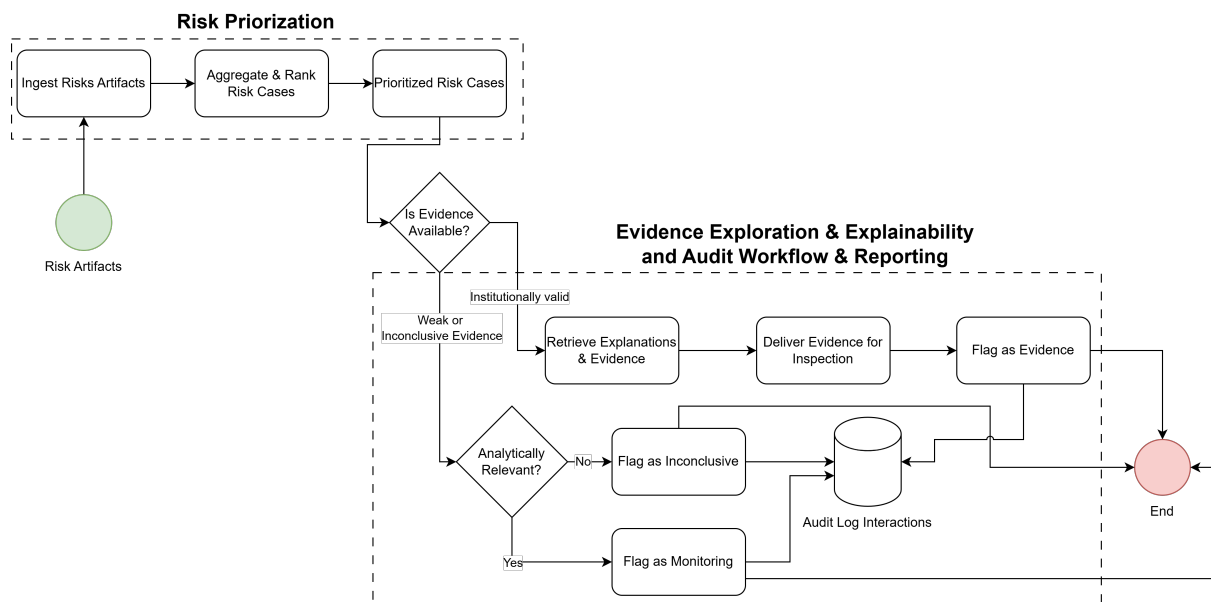


Figure 4.5: Decision Layer

The workflow begins with the ingestion of risk artifacts produced by the analytical components of the model, including red flags and aggregated risk indicators. These artifacts are subsequently combined and ranked into risk cases, allowing the system to prioritize procurement entities, procedures, or actors that exhibit higher concentrations of analytically identified risk. At this stage, prioritization serves exclusively as a mechanism for attention allocation and does not imply the existence of wrongdoing.

Once risk cases are prioritized, the workflow introduces a first decision point that evaluates whether supporting evidence is available. Evidence is understood as institutionally recognizable artifacts, such as procurement records, contractual documentation, transactional data, or audit relevant registries, that can substantiate or contextualize the identified risk signals. When no such evidence exists, or when available information is

insufficient, the case is explicitly classified as weak or inconclusive evidence, preventing analytically derived suspicion from being prematurely escalated.

When evidence is available, the Decision Layer structures the corresponding institutional records and contextual information associated with the prioritized case. This step does not generate new analytical interpretations; rather, it prepares the available material so that subsequent assessment is grounded in traceable and verifiable documentation. A second decision point then assesses whether the case remains analytically relevant given the retrieved evidence. This gate formalizes the possibility that a case may be analytically prioritized in earlier stages but lose relevance once examined in light of concrete data. If the case is deemed no longer analytically relevant, it is flagged as inconclusive, preserving the analytical trace while avoiding unnecessary escalation.

If the case is considered analytically relevant, but does not yet justify immediate inspection, it is flagged for monitoring. Monitoring flags indicate cases that warrant continued observation over time, enabling the accumulation of additional evidence or the detection of evolving risk patterns without triggering formal investigative procedures. For cases in which analytical relevance and evidentiary support converge, the workflow delivers the structured evidence to human inspectors. At this point, the Decision Layer provides a consolidated evidentiary package that supports formal inspection processes while preserving the primacy of professional judgment. Such cases are finally flagged as evidence, indicating readiness for institutional scrutiny rather than confirmation of fraud.

4.3.6 Ethical Layer

The Ethical Layer establishes the normative principles that guide the design and use of the reference model for PP oversight. While the core operational layers focus on data processing, analytical reasoning, and decision support functionalities, this layer defines the ethical boundaries and governance mechanisms within which such capabilities may be exercised. Conceptually, the Ethical Layer incorporates legal norms, institutional values, and ethical guidelines relevant to the use of data driven and AI based systems in the public sector, translating them into operational requirements that shape system behavior, human interaction, and traceability across the pipeline. By embedding ethical considerations as a transversal layer, the framework ensures that fraud risk analysis supports integrity, fairness, and legitimacy, while explicitly avoiding the automation of judgment in high stakes public decision contexts.

To operationalize these objectives, the Ethical Layer is structured around three in-

terrelated ethical principles: *Human Oversight*, *Transparency and Explainability*, and *Accountability*. The *Human Oversight* principle establishes that analytical outputs produced by the framework serve strictly as decision-support inputs, ensuring that auditors retain authority over interpretation, validation, and escalation. The *Transparency and Explainability* principle requires that data sources, analytical logic, and decision rationales be intelligible to human actors, enabling auditors to understand how indicators, assumptions, and declared data limitations contribute to risk characterizations. Finally, the *Accountability* principle affirms that responsibility for analytical choices, interpretations, and institutional actions remains with identifiable human actors and organizations. Together, these principles define the ethical conditions under which the reference model operates and ensure that ethical guarantees are operationalized through concrete, inspectable, and auditable system behaviors.

Figure 4.6 illustrates the Ethical Layer as a transversal governance structure that permeates the Data, Engine, and Decision layers of the proposed reference model. Rather than operating as an isolated or external control mechanism, the Ethical Layer embeds governance, transparency, and responsibility practices directly into the operational flow of fraud risk analysis. This design reflects the understanding that ethical principles in AI-supported public procurement oversight must be operationalized throughout the analytical lifecycle, from data preparation to analytical interpretation and institutional decision-making.

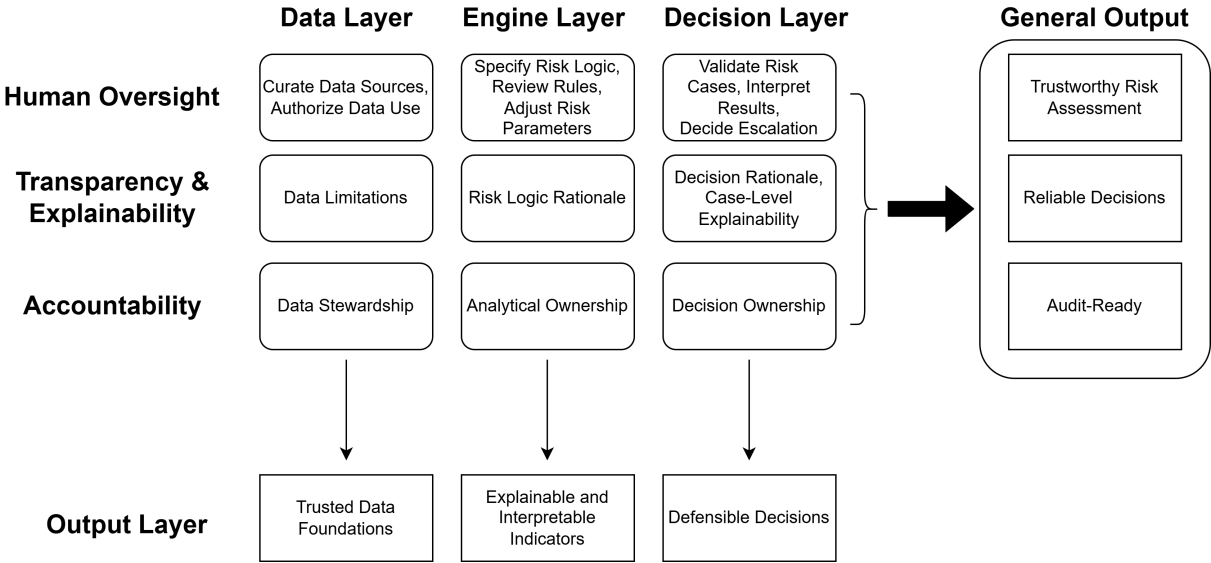


Figure 4.6: Ethical Layer

The figure is organized around three core ethical dimensions: *Human Oversight*,

Transparency and Explainability, and *Accountability*. These dimensions are directly aligned with the Trustworthy AI principles adopted in this thesis and discussed in Chapter 2, particularly the principles of *Respect for Human Autonomy* and *Explainability* proposed by the European Commission guidelines for Trustworthy AI. More specifically, *Human Oversight* and *Accountability* operationalize the principle of *Respect for Human Autonomy* by ensuring that analytical systems remain subject to meaningful human supervision, institutional control, and identifiable responsibility structures. Similarly, *Transparency and Explainability* operationalize the *Explainability* principle by enabling analytical processes, risk indicators, and decision-support outputs to remain understandable, interpretable, and contestable within public sector oversight environments.

At the Data Layer, the Ethical Layer establishes the governance conditions under which data can be legitimately collected, integrated, processed, and used for fraud risk analysis. Human oversight is exercised through the curation of data sources and authorization of data use, ensuring that datasets remain institutionally appropriate and aligned with legal and organizational constraints. Simultaneously, transparency and explainability mechanisms make explicit the limitations, scope, and contextual restrictions associated with the available data, preventing analytical misuse or overinterpretation of incomplete or low-quality information. Accountability is reinforced through data stewardship practices that associate datasets, transformations, and preprocessing activities with identifiable institutional actors and responsibilities. Collectively, these mechanisms contribute to the establishment of trusted data foundations capable of supporting analytically robust, institutionally legitimate, and ethically governed fraud risk analysis processes.

At the Engine Layer, the Ethical Layer governs how analytical logic is constructed, interpreted, and maintained. Human actors are responsible for specifying risk logic, reviewing rules, and adjusting analytical parameters according to institutional needs and contextual knowledge. Simultaneously, transparency mechanisms expose the rationale behind risk logic and indicator construction, while accountability is reinforced through analytical ownership and the explicit attribution of responsibility for the implemented models, rules, and analytical procedures. This structure seeks to prevent the delegation of interpretive authority to opaque or autonomous systems by ensuring that analytical behavior remains understandable and institutionally controllable.

At the Decision Layer, ethical governance is materialized through the validation of risk cases, interpretation of analytical results, and escalation decisions performed by auditors or public officials. Explainability mechanisms support decision rationales and case-level

interpretability, enabling users to understand why specific contracts, suppliers, or procurement processes were analytically prioritized. Accountability is further reinforced through decision ownership, ensuring that institutional actions remain attributable to identifiable actors rather than to the system itself.

Building upon these ethical mechanisms, this thesis also incorporates a procedural perspective for the operationalization of ethical principles in AI-supported fraud risk analysis. In particular, the proposed Ethical Layer is complemented by an ethical governance pipeline for fraud detection in public procurement previously developed and published by the author in (SAMPAIO; DE OLIVEIRA ANDRADE, et al., 2026). While the Ethical Layer defines how ethical principles are structurally embedded across the Data, Engine, and Decision layers, the ethical pipeline complements this perspective by operationalizing how these principles should be implemented during the development and deployment of AI-based solutions for fraud detection in public procurement.

The ethical pipeline incorporated into this thesis was derived from a focused analytical study conducted from the SLR I Chapter 3. More specifically, the study analyzed the intersection between the Trustworthy AI principles adopted in this thesis and the ethical challenges reported in the literature on AI-supported fraud detection in PP (SAMPAIO; BERNARDINI; VITERBO, 2024). As a result, five recurring ethical vulnerabilities were identified and structured into operational ethical subprocesses that guide how ethical principles should be implemented throughout the development and deployment lifecycle of AI-based fraud detection solutions. The five challenges are:

- **E1. Lack of Strategic Control:** The absence of a comprehensive governance framework for using AI in PP fraud detection. Many AI-driven fraud detection systems can be implemented without clear guidelines on their objectives, limitations, and integration into existing procurement oversight structures (OKO-ODION, 2025). This lack of strategic oversight can result in inconsistent adoption across different governmental agencies, fragmented enforcement mechanisms, and potential misuse of AI-generated risk scores (ADEPOJU; CHINONYEREM, 2025). Furthermore, AI models may be deployed without a clear strategy or assessment of their long-term societal and legal impacts, leading to ethical and operational risks. To ensure effective and responsible AI deployment, PP agencies must establish strategic governance structures that define how AI should be used, monitored, and aligned with broader policy objectives (ADEWUSI et al., 2024).
- **E2. Limitations in Explainability Tools:** Explainability tools provide insights

into AI decision-making, helping users understand why a model classifies certain procurement transactions or suppliers as fraudulent. However, these tools have significant limitations, particularly when applied to highly regulated environments such as PP. Methods such as SHAP (Shapley Additive Explanations) (LUNDBERG; LEE, 2017) and LIME (Local Interpretable Model-agnostic Explanations) (RIBEIRO; SINGH; GUESTIN, 2016) are commonly used to generate explanations. Still, they can be overly technical, inconsistent across different models, or fail to provide actionable insights for policymakers. Additionally, explainability techniques often prioritize mathematical coherence over legal and procedural clarity, making them inadequate for government officials who need concrete, legally defensible justifications. If explainability tools are not robust enough, procurement fraud detection systems risk becoming ineffective, unaccountable, and difficult to challenge in cases of erroneous flagging. Therefore, developing explainability frameworks tailored to PP regulations is essential, ensuring that AI-generated justifications align with governance requirements.

- **E3. Lack of Transparency for Users:** Limited access to information about how AI models operate, what factors influence their decisions, and how procurement officials should interpret their outputs (ADENIRAN; ONEBUNNE; WILLIAM, 2024). In PP fraud detection, AI tools are often used by auditors and government officials who may not have technical expertise in ML, making it difficult for them to understand how AI-based systems arrive at specific fraud risk assessments. This opacity can lead to misuse of AI predictions, where procurement officials either unquestioningly trust the model's outputs or disregard them due to a lack of comprehension. Furthermore, affected suppliers and contractors may face restrictions or penalties without a clear explanation, potentially undermining the fairness and legitimacy of procurement decisions. To mitigate this issue, AI systems used in PP must be designed with clear (SHAHRIAR et al., 2023), user-friendly interfaces that provide insights into how fraud risks are assessed, ensuring that users can critically engage with the AI-driven decision-making process.
- **E4. Lack of Oversight During Operation:** When AI-based fraud detection systems operate without continuous human monitoring, validation, or the ability to override automated decisions. In the PP domain, AI models are often trained on historical data, which may fail to capture evolving fraud tactics or changes in procurement regulations. Without ongoing oversight, these systems can drift in accuracy, reinforce outdated biases, or generate misleading risk assessments (OKO-ODION,

2025), leading to missed fraud cases or false positives that unfairly penalize suppliers. These false positives are particularly critical, as they stem from model-driven decisions and may expose suppliers to reputational harm, even in the absence of confirmed wrongdoing. Additionally, government procurement processes require human accountability, meaning that an AI system alone cannot determine the validity of a transaction without human review. Ensuring oversight in AI-driven fraud detection requires establishing mechanisms for periodic auditing, model recalibration, and human intervention, allowing auditors to challenge or validate AI-generated alerts in real time.

- **E5. System Opacity (Black Box):** System opacity refers to the lack of interpretability in AI models, particularly in complex ML systems such as deep learning and ensemble methods. In fraud detection for PP, opacity becomes a significant challenge when AI models flag transactions, suppliers, or bidding patterns as suspicious without clear justifications. PP processes require audibility and justifiability, as government agencies must explain their decisions (HICKOK, 2024). However, opaque AI models can erode trust among auditors, procurement officers, and external stakeholders, who may struggle to understand why certain entities are flagged for investigation. The inability to scrutinize AI-driven decisions can also hinder legal compliance (SPULBAR, 2025), as PP is subject to strict regulations that demand transparency in decision-making. Ensuring that AI models are not “black boxes”, but interpretable systems is essential to maintaining accountability and due process in procurement oversight.

Figure 4.7 presents a schematic view of PRO-Trust pipeline, highlighting the main Tasks (T1-T7) of the process and the associated Ethical Challenges (E1-E5). The pipeline begins with the data collection and red flag definition task (T1), followed by data labeling (T2), model selection (T3), testing (T4), and evaluation (T5). If the model meets the required metrics, it advances to production (T6) and subsequently to the alerts and notifications phase (T7). We mapped the Ethical Challenges E1-E5 as subprocesses. E1 – Lack of Strategic Control occurs even before data is obtained, reflecting the absence of a well-defined governance framework for AI use. Then, before the production phase, E2 – Limitations in Explainability Tools highlights the challenges of interpreting the model’s decisions, which directly influence auditors’ and regulators’ confidence.

Additionally, E3 – Lack of Transparency for Users highlights that, even if a model is interpretable, its outputs must be understandable to non-technical users, enabling au-

ditors and managers to make informed decisions. After implementation, E4 – Lack of Oversight During Operation – arises, where the lack of continuous monitoring can lead to outdated models and erroneous decisions. Finally, E5 – System Opacity represents the risk that the model becomes a “black box”, making audits and justifications for the decisions made difficult. Given this pipeline, in which each ethical aspect is integrated as a subprocess within the AI pipeline for fraud detection in PP, we also examine how each subprocess operates. This in-depth analysis provides a structured approach to embedding ethical considerations directly into the AI workflow, ensuring greater transparency, accountability, and reliability in real- world applications.

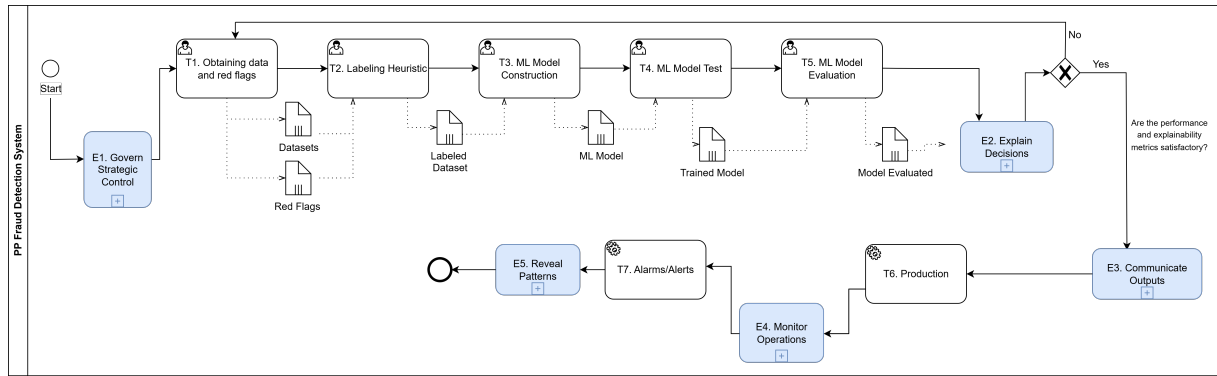


Figure 4.7: Our ethics-oriented pipeline for constructing trustworthy AI-based fraud detection systems for PPs. It supports the research objective of embedding ethical safeguards directly into the AI workflow, linking each stage to identified challenges.

Figure 4.8 presents the proposed subprocess to address the ethical aspect E1 - Lack of Strategic Control, which refers to the lack of explicit strategic control over using AI systems for fraud detection in PP. This flow of activities begins with the definition of the strategic objectives of the fraud detection system (E1.1), followed by the elaboration of transparency, ethics, and compliance guidelines (E1.2). Next, the ethical and technical limits of the solution are defined (E1.3), as well as a survey of applicable laws and regulations (E1.4), such as LGPD, anti-corruption standards, and trustworthy AI guidelines. Step E1.5 assesses risks associated with AI use, and the results determine whether the process can proceed. If the risks are considered acceptable, the flow advances to the definition of bias monitoring metrics over time (E1.6), ensuring the continuous alignment of the system with the established strategic and ethical objectives. It is essential to highlight that the flow foresees review cycles, allowing a return to previous stages if risks are high or metrics do not meet strategic control requirements, thus promoting an iterative process of responsible governance.

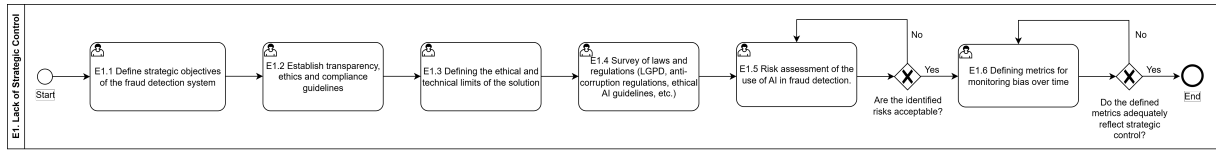


Figure 4.8: E1: Lack of strategic control. This subprocess illustrates how the proposed framework addresses the absence of governance and long-term oversight in AI-based fraud detection.

Figure 4.9 represents the proposed subprocess to mitigate the ethical aspect E2. Limitations in Explainability Tools, related to the limitations of explainability techniques applied to AI systems used to fraud detection in PP. The process begins by applying interpretability techniques (E2.1), such as SHAP, LIME, and other approaches that generate explanations of the model's decisions. The explanations generated are then compared with legal and regulatory requirements (E2.2) to ensure compliance with current standards, such as the General Data Protection Law (LGPD) and other guidelines on the transparency and justifiability of automated decisions. Suppose the explanations violate any legislation or do not comply with regulatory requirements. In that case, the process foresees a return to the initial stage to adjust the techniques applied, promoting an iterative cycle of continuous improvement. If, on the other hand, the explanations are adequate, the subprocess is completed, ensuring that the AI system operates in a more transparent, auditable, and legally secure way.

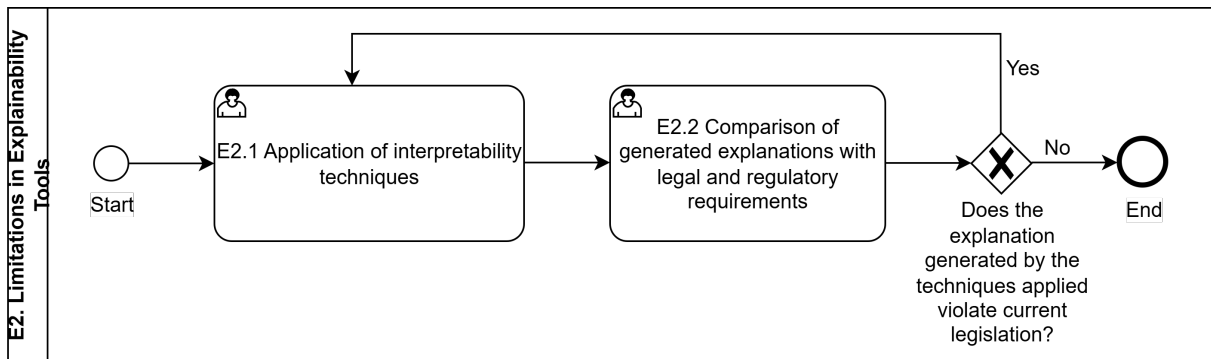


Figure 4.9: E2: Limitations in explainability tools. This subprocess shows how the framework mitigates technical and legal shortcomings of current explainability methods.

Figure 4.10 illustrates the proposed subprocess to address the ethical aspect E3. Lack of Transparency for Users, which refers to the difficulty users, such as auditors and public managers, have in understanding and correctly using the output generated by AI systems for fraud detection in PP. The process begins with usability testing (E3.1), which aims to verify whether auditors and public agents can interpret the information and alerts issued

by the model. Next, accessible documentation is developed (E3.2), clearly explaining how the AI system assesses risks, what criteria it uses, and how non-technical users should interpret the results. Finally, the subprocess foresees the creation of a feedback form (E3.3) that allows users to report difficulties or questions regarding the alerts they receive, enabling continuous improvement in system communication. In this way, the flow aims to ensure that AI-based solutions are understandable, transparent, and useful for decision-making in PP, thereby promoting trust and responsible use of technology.

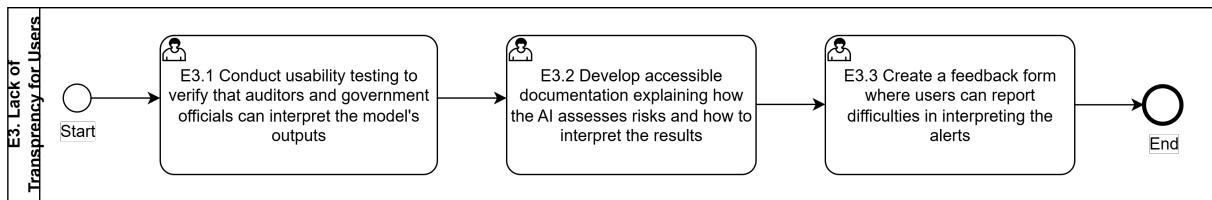


Figure 4.10: E3: Lack of transparency for users. This subprocess demonstrates how the framework improves user-facing communication and understanding of AI outputs in PP.

Figure 4.11 describes the proposed subprocess to mitigate ethical aspect E4. Lack of Oversight During Operation, related to the absence of continuous human monitoring and review mechanisms in the automated decisions of AI systems applied to fraud detection in PP. The flow begins by creating an audit committee (E4.1) composed of experts who periodically review the AI-generated predictions. Next, a mandatory human review process (E4.2) is established for all high-risk alerts, ensuring that no relevant decision occurs without due human intervention. In addition, the subprocess includes implementing a feedback system (E4.3), which allows auditors to classify alerts as applicable or misleading, contributing to the continuous improvement of the model. To ensure real-time monitoring, a continuous dashboard (E4.4) is planned to track the model's performance and identify deviations. In addition, criteria are defined for periodic reviews and recalibration of the model (E4.5) whenever a significant variation in performance is detected. Finally, the subprocess includes creating a formal dispute mechanism (E4.6) that allows impacted suppliers to question decisions based on AI system alerts. This set of steps aims to ensure that AI in fraud detection is always under human supervision, promoting error correction, continuous learning, and respect for the rights of those involved.

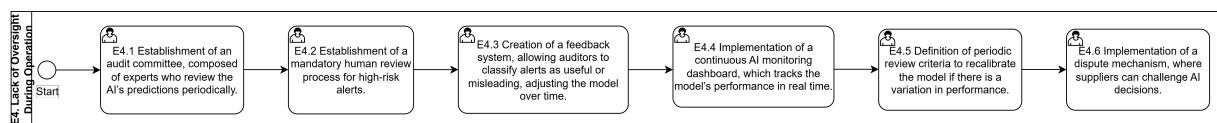


Figure 4.11: E4: Lack of oversight during operation. This subprocess highlights mechanisms to ensure continuous human monitoring and intervention in AI-supported auditing.

Figure 4.12 presents the proposed subprocess to mitigate the ethical aspect E5. System Opacity (Black Box) addresses the lack of transparency and interpretability of AI systems used for fraud detection in PP. This flow begins by implementing an explanatory layer mechanism (XAI) (E5.1), which aims to translate the AI’s decisions into understandable justifications for users. Next, the development of explanations in accessible language (E5.2) is planned, aimed at auditors and public managers, and highlights the main factors that led to the signaling of fraud risk, such as anomalous pricing patterns or atypical supplier behavior. Finally, the subprocess includes the integration of an interactive audit dashboard (E5.3), allowing auditors to transparently verify and consult the criteria and variables used in each system decision. With this, the flow seeks to break with the “black box” logic of AI models, promoting greater trust, auditability, and the ability to challenge automated decisions.

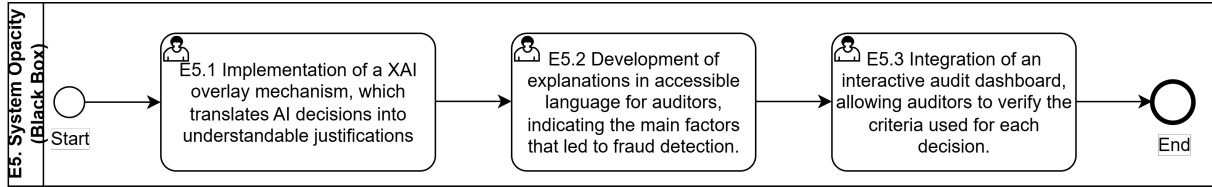


Figure 4.12: E5: System opacity (black box). This subprocess illustrates how the framework reduces black-box risks by integrating explanatory layers and interactive audit dashboards.

4.3.7 Provenance Layer

The *Provenance Layer* represents the traceability and reproducibility dimension of the proposed reference model. In the context of AI-supported fraud risk analysis in PP, provenance is understood as the capability to document, reconstruct, inspect, and audit the complete lifecycle of data transformations, analytical processes, and decision-support activities. Provenance mechanisms allow institutional actors to identify the origin of datasets, understand how analytical outputs were produced, trace the execution of rules and models, and reconstruct the sequence of actions that led to specific risk assessments or institutional decisions.

Although provenance is discussed in the literature as an ethical component associated with explainability, transparency, and trustworthy AI (KALE et al., 2023), this thesis deliberately treats provenance as a distinct architectural layer rather than merely as a subdimension of the Ethical Layer. Recent studies argue that provenance documentation plays a central role in enabling explainable and trustworthy AI systems by

supporting transparency, reproducibility, accountability, and auditability throughout AI workflows (KALE et al., 2023; WERDER; RAMESH; ZHANG, 2022; BENMOHAMED; SHEN; VLAHU-GJORGIEVSKA, 2024; CHAWLA, 2021). However, in this reference model, provenance is positioned as an independent cross-layer capability because its function extends beyond ethical governance alone. Provenance operates as a foundational infrastructural mechanism that supports analytical traceability, workflow reconstruction, institutional auditing, and reproducibility across the entire lifecycle of fraud risk analysis processes. This distinction allows provenance to be conceptualized not only as an ethical enabler, but also as a technical and organizational mechanism for institutional control and analytical governance.

Figure 4.13 presents the Provenance Layer of the reference model. The figure illustrates how provenance mechanisms permeate the three operational layers of the architecture — *Data*, *Engine*, and *Decision*. In the *Data Layer*, provenance is operationalized through source provenance and pipeline lineage mechanisms, enabling datasets, transformations, and integration procedures to remain traceable and institutionally documented. In the *Engine Layer*, provenance supports model and rule reproducibility by recording analytical logic, parameter configurations, rule versions, and execution contexts associated with risk computation processes. In the *Decision Layer*, provenance is materialized through decision traceability mechanisms that connect analytical outputs with human interpretations, validation actions, and institutional escalation procedures.

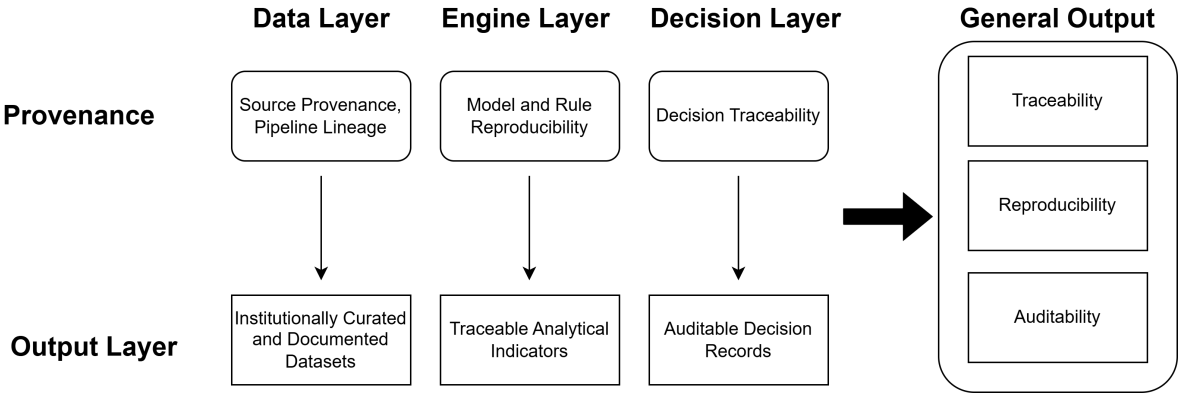


Figure 4.13: Provenance Layer

The outputs generated by these provenance mechanisms differ according to each operational layer. At the Data Layer, provenance contributes to the generation of institutionally curated and documented datasets, ensuring that data origins, transformations, and preparation procedures remain inspectable and reproducible. At the Engine Layer, provenance supports the production of traceable analytical indicators, allowing auditors

and analysts to reconstruct how risk scores, red flags, and prioritization outputs were generated. At the Decision Layer, provenance enables auditable decision records, linking analytical evidence to institutional interpretations, validation actions, and investigative decisions. Collectively, these outputs contribute to broader organizational capabilities associated with analytical traceability, reproducibility, and audit-ready oversight.

4.3.8 Evaluation and Refinement Layer

The Evaluation and Refinement Layer is responsible for the continuous assessment and refinement of the reference model once it is in use, ensuring that analytical logic, data inputs, and decision support outcomes remain aligned with institutional objectives, regulatory constraints, and operational realities. Unlike the core operational layers, which focus on producing risk assessments and supporting audit activities, the Evaluation Layer introduces a reflexive mechanism that enables the reference model to learn from its own use. By systematically incorporating auditor feedback, monitoring analytical behavior, and recalibrating indicators and thresholds, this layer ensures that the reference model evolves in a controlled, evidence-based, and institutionally grounded manner. In this sense, the Evaluation Layer operationalizes continuous improvement as a governance function rather than a purely technical optimization task.

To fulfill this role, the Evaluation and Refinement Layer is structured around three complementary activities: *Auditor Feedback Collection*, *Indicator Calibration and Threshold Tuning*, and *Model Evaluation and Monitoring*. Auditor Feedback Collection captures experiential knowledge generated during the use of the reference model, including perceptions of data adequacy, indicator usefulness, and decision support utility. Indicator Calibration and Threshold Tuning translate this feedback into concrete adjustments to risk logic, weights, and decision thresholds, ensuring alignment with institutional risk tolerance and audit priorities. Model Evaluation and Monitoring extend this process by continuously assessing whether analytical logic, indicators, and underlying assumptions remain appropriate in light of regulatory changes, evolving procurement practices, and shifts in data availability. Together, these activities prevent analytical stagnation and ensure that the reference model remains responsive to both institutional learning and contextual change.

Figure 4.14 illustrates how the Evaluation and Refinement Layer intersects with the Data, Engine, and Decision layers, embedding continuous assessment mechanisms throughout the analytical pipeline. In the interaction with the Data Layer, evaluation

focuses on data coverage, relevance, and the broader data landscape, enabling auditors and analysts to assess whether existing sources remain adequate and to identify opportunities for incorporating new or complementary datasets. These activities support the validation and evolution of the data environment, ensuring that analytical inputs remain institutionally legitimate and analytically meaningful.

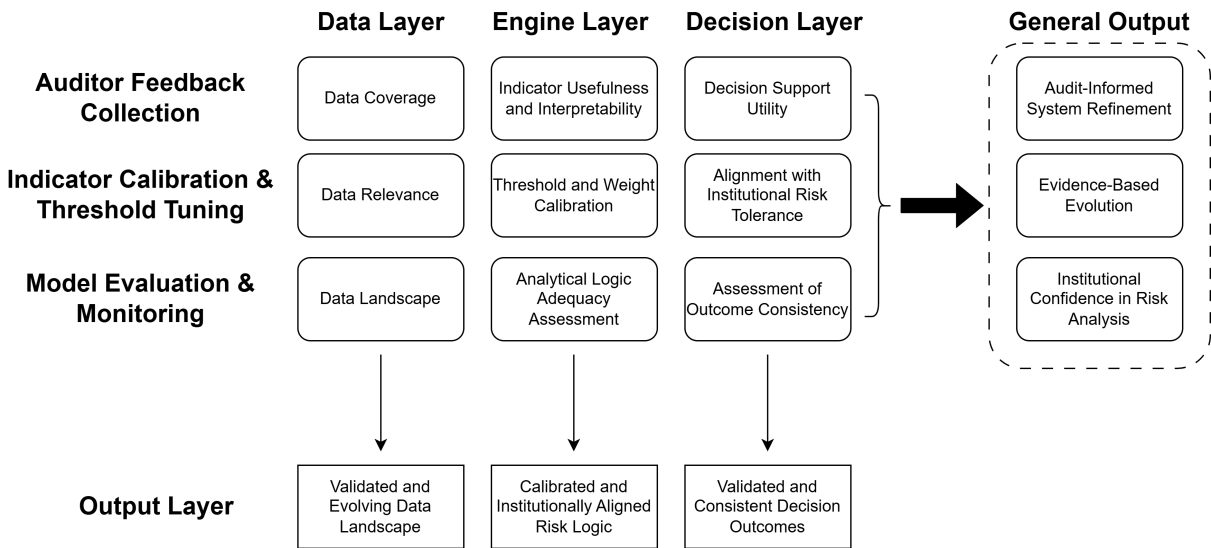


Figure 4.14: Evaluation and Refinement Layer

In the interaction with the Engine Layer, evaluation addresses the usefulness, interpretability, and adequacy of risk indicators and analytical logic. Feedback-driven calibration of thresholds and weights allows risk scores to remain aligned with institutional priorities, while periodic reassessment of analytical logic enables the reference model to adapt to regulatory changes, evolving procurement practices, or emerging fraud patterns.

At the Decision Layer, evaluation mechanisms examine the practical utility of decision-support outputs, including their alignment with institutional risk tolerance and the consistency of outcomes over time. By assessing whether analytically prioritized cases support coherent audit decisions and escalation practices, this interaction helps ensure that analytical outputs translate into stable and defensible decision-support results.

Overall, the Evaluation and Refinement Layer does not produce new analytical decisions but generates refined institutional artifacts across the system. At the Data Layer, it contributes to a validated and evolving data landscape; at the Engine Layer, to calibrated and institutionally aligned risk logic; and at the Decision Layer, to consistent decision support outcomes. Collectively, these processes support the continuous evolution of the reference model and reinforce its long-term reliability for public procurement

oversight.

4.3.9 Governance and Security Layer

The Governance and Security Layer defines the institutional and technical foundations that enable the secure, controlled, and accountable operation of the proposed reference model within public sector environments. Conceptually, the Governance and Security Layer consumes organizational policies, legal constraints, and role definitions associated with public procurement oversight, and produces enforceable security and governance mechanisms that regulate user interactions and system behavior. By embedding security and governance concerns as transversal elements, this layer ensures that analytical capabilities are exercised in accordance with institutional mandates, safeguarding sensitive data, preserving auditability, and maintaining trust in the reference model's operation.

To operationalize these objectives, the Governance and Security Layer is composed of three tightly integrated components: *Role-Based Access Control (RBAC)*, *Logging*, and *Security Controls*. The *RBAC* component regulates access to data assets, analytical functions, and decision support features by assigning permissions based on clearly defined organizational roles, such as data engineers, data scientists, and auditors. This mechanism ensures that users interact with the reference model strictly within the boundaries of their institutional responsibilities. The *Logging* component provides systematic recording of user actions, data access events, and analytical executions, creating an auditable trail that supports accountability, incident investigation, and compliance verification. Finally, the *Security Controls* component encompasses technical safeguards designed to protect the reference model against unauthorized access, data leakage, and operational misuse, including secure execution environments, integrity checks, and monitoring of anomalous system behavior. Collectively, these components enforce governance and security requirements across all layers of the reference model, ensuring lawful data handling, controlled usage, and robust protection of analytical processes in public procurement oversight contexts.

Figure 4.15 illustrates how governance and security mechanisms permeate the Data, Engine, and Decision layers of the reference model. At the Data Layer, RBAC regulates data access, logging records data usage and processing activities, and security controls ensure data protection and integrity. Together, these mechanisms produce secure and institutionally governed data assets, ensuring that sensitive procurement data and derived datasets can be safely used for analytical purposes.

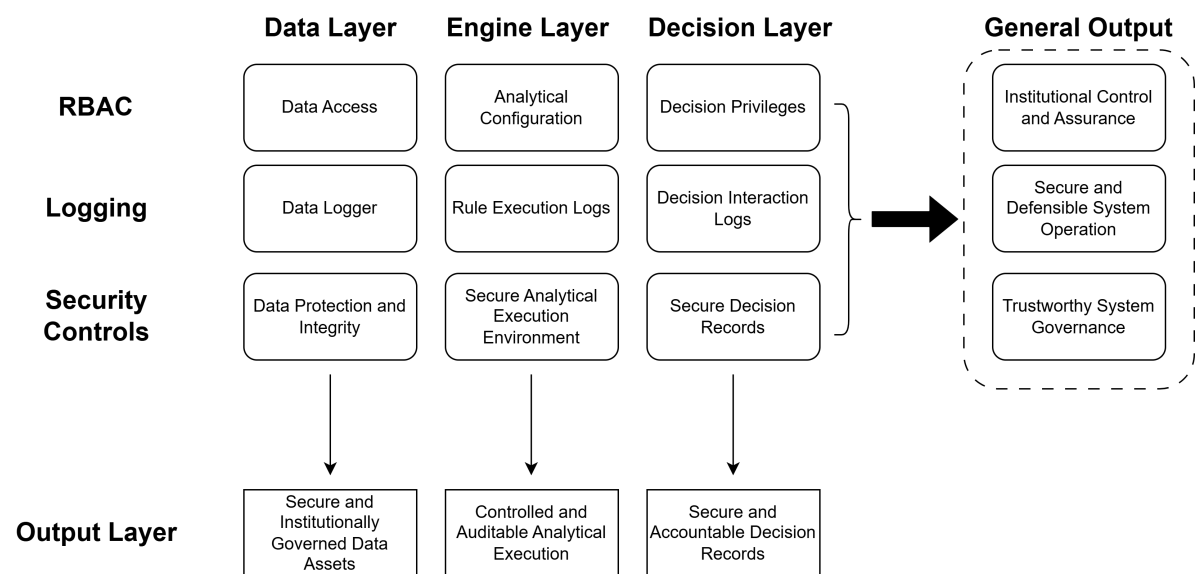


Figure 4.15: Governance and Security Layer

At the Engine Layer, governance and security mechanisms regulate analytical configuration through role-based privileges, record rule execution and analytical processing logs, and protect the analytical execution environment against unauthorized changes. This interaction ensures that risk logic, indicators, and scoring mechanisms are executed in a controlled and auditable manner, resulting in controlled and auditable analytical execution.

At the Decision Layer, RBAC defines decision privileges and escalation authority, logging captures interactions with decision-support outputs, and security controls protect decision records. These mechanisms ensure that analytically supported decisions remain traceable, protected, and institutionally accountable, resulting in secure and accountable decision records without automating or obscuring human responsibility.

The outputs generated by the Governance and Security Layer are not analytical results, but institutional guarantees that enable sustainable and defensible system operation. At the Data, Engine, and Decision layers, this layer produces secure and institutionally governed data assets, controlled and auditable analytical execution, and secure and accountable decision records, respectively. Collectively, these outputs contribute to a set of General Outputs that reflect institutional maturity and operational robustness, including institutional control and assurance, secure and defensible system operation, and trustworthy system governance. These outcomes ensure that the reference model can be safely integrated into public procurement oversight practices and withstand internal and external scrutiny over time.

4.4 Final Remarks

This chapter presented the conceptual design of the proposed reference model for fraud risk analysis in PP, detailing the architecture and the set of analytical and institutional artifacts that compose it. Grounded in the DSR paradigm, the chapter articulated how the reference model structures the transformation of heterogeneous government data into interpretable risk indicators and decision support artifacts. By defining the components, interactions, and responsibilities embedded in the architecture, the chapter establishes the design blueprint that operationalizes the analytical and governance principles guiding the proposed solution.

At the core of this architecture are three operational layers that structure the analytical pipeline: the *Data*, *Engine*, and *Decision* layers. The Data Layer is responsible for identifying, acquiring, and harmonizing heterogeneous public datasets, transforming raw institutional data into refined analytical inputs. The Engine Layer constitutes the analytical core of the framework, where different forms of risk reasoning, heuristic rules, analytical procedures, and AI based methods, are combined to generate interpretable fraud risk indicators. The Decision Layer translates these analytical artifacts into auditor centered decision support mechanisms, enabling case prioritization, evidence exploration, and structured interaction with risk assessments while preserving human judgment and institutional accountability.

Complementing these operational components, the architecture incorporates transversal layers that ensure the reference model's responsible and sustainable operation. The Ethical Layer establishes normative principles such as human oversight, transparency, explainability, accountability, and provenance, ensuring that analytical processes remain interpretable and contestable. The Governance and Security Layer introduces the organizational and technical safeguards required for secure data management, controlled access, and auditable system operation. Finally, the Evaluation and Refinement Layer embeds continuous feedback and learning mechanisms that allow the framework to evolve through auditor input, changes in data availability, and shifts in regulatory or institutional contexts. Together, these transversal layers transform the reference model into a sociotechnical artifact capable of supporting trustworthy and institutionally grounded fraud risk analysis in PP.

Chapter 5

Applying the reference model

This chapter presents the instantiation of the proposed reference model for fraud risk analysis in PP. While the previous chapter introduced the conceptual architecture and design principles underlying the artifact, the objective here is to demonstrate how each layer can be operationalized in a concrete context. Within the DSR paradigm, instantiation represents a crucial step for demonstrating the practical applicability of a designed artifact. In this sense, the chapter aims to (i) operationalize the components of the reference model within a real PP data ecosystem and (ii) illustrate how the proposed model can support fraud risk analysis through the transformation of heterogeneous government data into open, structured and interpretable risk indicators. Part of the operationalization process presented in this chapter builds upon previous work conducted by the author on the construction of public procurement risk indicators from OGD and provenance-aware analytical pipelines (SAMPAIO; BERNARDINI; VITERBO, et al., 2026), particularly regarding the integration of heterogeneous datasets, the definition of red flags, and the explicit modeling of traceability across the indicator–data–source lifecycle.

The primary empirical context used for instantiation is the Brazilian PP ecosystem, which provides a rich landscape of OGD sources relevant to fraud risk analysis. Through this instantiation, the chapter illustrates how the Data, Engine, Decision, Ethical, and Governance and Security layers of the reference model can be configured to transform government data into structured and interpretable fraud risk indicators. By grounding the architecture in a concrete data ecosystem, the chapter demonstrates the practical feasibility of the proposed design and clarifies how its components interact within an operational analytical pipeline.

The remainder of the chapter is structured according to the layers of the reference

model. The following sections describe the instantiation of the Data Layer, Engine Layer, Decision Layer, Ethical Layer, Provenance and Governance and Security Layer within the Brazilian context. The Evaluation and Refinement Layer, which introduces mechanisms for continuous learning, feedback integration, and institutional calibration of the model, is examined separately in Chapter 6, where the evaluation of the artifact and its implications for iterative improvement are discussed.

5.1 Data Layer

The Data Layer constitutes the foundational component of the reference model, as it is responsible for enabling the systematic acquisition and preparation of data. In the context of the present instantiation, this layer operationalizes the processes through which heterogeneous government data sources are identified, collected, and transformed into refined data suitable for subsequent analytical processing. In the Brazilian case examined in this chapter, these sources primarily consist of open government data (OGD). However, the reference model does not assume that procurement data must necessarily be open, as in many institutional contexts relevant datasets may only be accessible through restricted governmental systems or controlled databases. Given the fragmented and heterogeneous nature of public procurement data ecosystems, particularly in the Brazilian context, the Data Layer plays a critical role in establishing a coherent and reproducible data infrastructure capable of supporting downstream analytical activities.

Data sources were selected to ensure reliable and comprehensive coverage of Brazil's PP, prioritizing public datasets released under open data policies. The data structure integrates ten official datasets that cover different stages of the PP process and related administrative domains. The Transparency Portal (D1) ¹ provides data on public expenditures, including detailed payment records from social programs such as Bolsa Família (D2) ². The Superior Electoral Court (D3) ³ dataset contains information on candidates, political parties, campaign donations, and election results. The Government Procurement Portal (CATMAT/CATSER) (D4) ⁴ lists goods and services procured by the federal government, while the ComprasNet Contracts API (D5) ⁵ provides records of tenders, contracts, sup-

¹<https://portal.datatransparencia.gov.br/>

²<https://portal.datatransparencia.gov.br/download-de-dados/bolsa-familia-pagamentos>

³<https://dadosabertos.tse.jus.br/dataset/>

⁴<https://www.gov.br/compras/pt-br/aceso-a-informacao/consulta-detalhada/planilha-catmat-catser>

⁵<https://contratos.comprasnet.gov.br/api/docs>

pliers, and contract values. The National Registry of Legal Entities (CNPJ) (D6) ⁶ offers company registration data and identifiers, and the Accounts System of the Federal Court of Accounts (TCU) (D7) ⁷ compiles institutional accounting and audit information. The Registry of Suspended and Debarred Companies (CEIS) (D8) ⁸ and the National Registry of Punished Companies (CNEP) (D9) ⁹ both contain lists of suppliers sanctioned by oversight bodies. The Transparency Portal – Invoices ¹⁰ (D10) includes invoice-level data on contract execution, and the Safra Guarantee Program (D11) ¹¹ dataset provides records of financial transfers to rural producers. Collectively, these data sets constitute a comprehensive and auditable basis for analyzing procurement activities using OGD.

Data were acquired from multiple Brazilian OGD sources. As illustrated in Figure 5.1, data acquisition was automated through Python scripts within a scalable cloud environment. The architecture is organized into three main layers. In the computing layer, Python and PySpark were executed on Amazon EMR to perform extraction, normalization, validation, and identifier harmonization procedures. Raw datasets were first ingested into an Amazon S3 landing zone, where they were preserved in their original format. Subsequently, transformation and integration routines were applied through a structured data engineering pipeline, generating harmonized datasets stored in a refined zone using Parquet format. The final processed datasets constitute the analytical data layer used for red flag generation. All code artifacts were version controlled and managed through a dedicated GitHub repository ¹², forming a distinct code layer that ensures reproducibility, transparency, and traceability across the entire data pipeline.

⁶<https://dados.gov.br/dados/conjuntos-dados/cadastro-nacional-da-pessoa-juridica---cnpj>

⁷<https://contas.tcu.gov.br/ords/f?p=1660:2:::N0:::>

⁸<https://portaldatransparencia.gov.br/download-de-dados/ceis>

⁹<https://portaldatransparencia.gov.br/download-de-dados/cnep>

¹⁰<https://portaldatransparencia.gov.br/download-de-dados/notas-fiscais>

¹¹<https://portaldatransparencia.gov.br/download-de-dados/garantia-safra>

¹²https://github.com/s-fontes/projeto_capivara

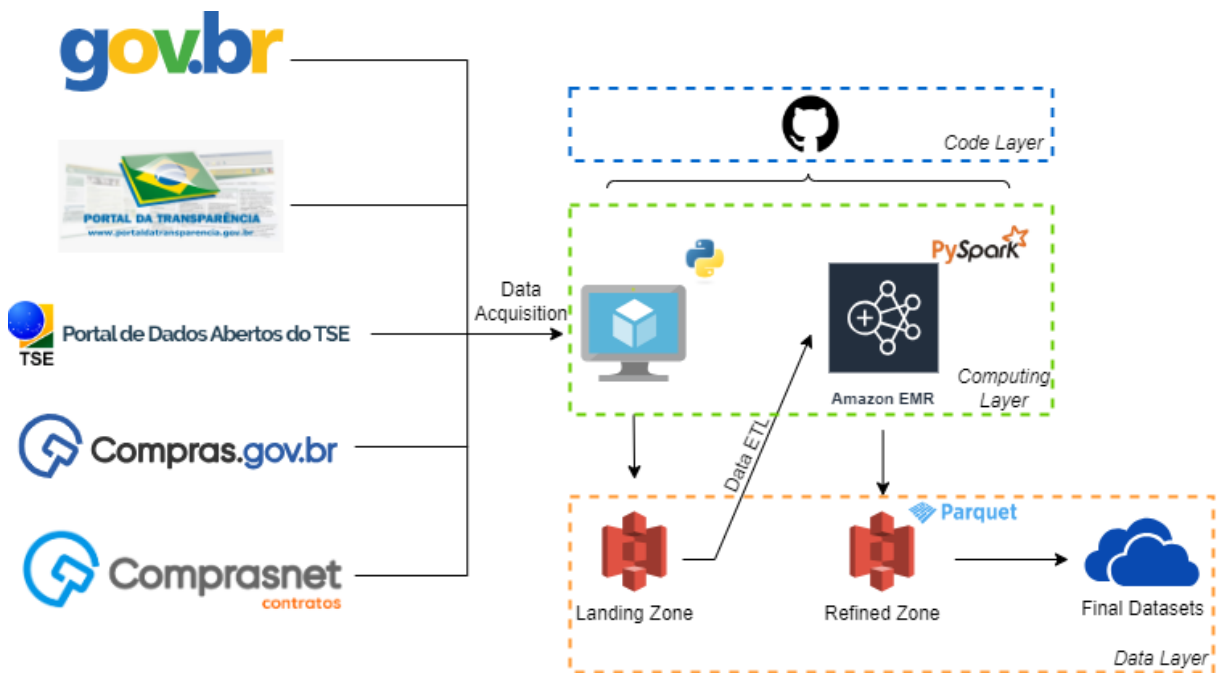


Figure 5.1: Data Extraction and Preparation Architecture

As the final output of the Data Layer, the datasets described above were integrated into a unified data model representing the core entities of the PP ecosystem. Figure 5.2 illustrates the Entity Relationship Model (ERM) of the resulting dataset, which consolidates procurement processes, suppliers, contracts, and related administrative records into a coherent refined structure. This data model represents the refined data layer within the data lake architecture, where previously ingested raw datasets are harmonized, linked, and structured to ensure consistency and analytical usability. The resulting modeled dataset therefore constitutes the refined data foundation that feeds the subsequent Engine Layer, enabling the computation of fraud risk indicators and other analytical mechanisms.

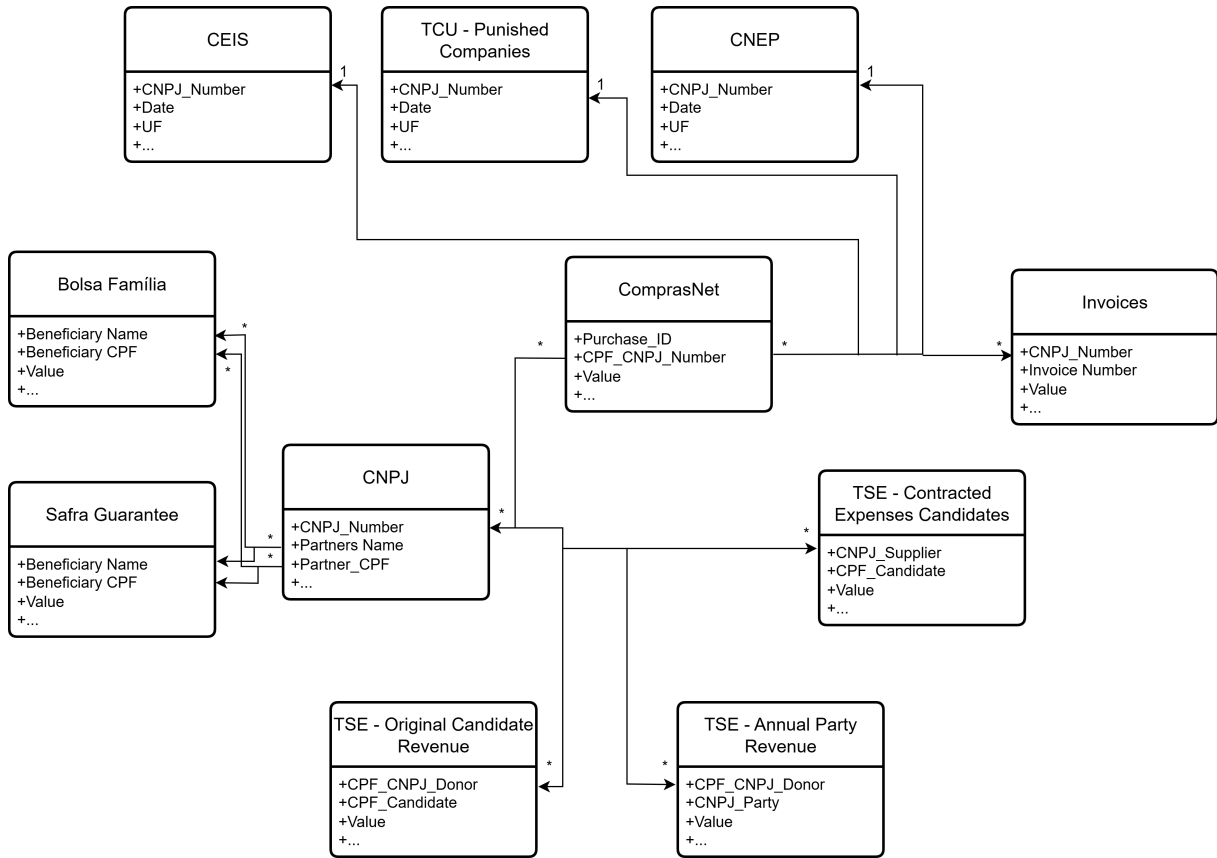


Figure 5.2: Data Relationship Model of the Refined Data Layer

5.2 Engine Layer

The Engine Layer constitutes the analytical core of the proposed reference model, where refined procurement data are transformed into interpretable risk indicators capable of supporting fraud risk analysis. Building upon the modeled dataset generated in the Data Layer, this layer operationalizes different forms of analytical reasoning designed to detect patterns, inconsistencies, and signals associated with potentially irregular procurement activities. In the context of the present instantiation, the Engine Layer combines complementary analytical mechanisms, including heuristic red flag rules, statistical and analytical procedures, and machine learning techniques, to systematically evaluate procurement entities and characterize their associated risk profiles.

5.2.1 Heuristics and Analytical Approach

The heuristics and analytical approach constitutes the first operational component of the Engine Layer, where domain knowledge derived from PP auditing practices and the liter-

ature review is translated into computable indicators of fraud risk. In this stage, the red flags identified in the literature and in institutional oversight practices are operationalized as measurable variables that capture observable signals associated with potentially irregular procurement behavior. These indicators are subsequently evaluated through rule based logic and statistical procedures designed to detect anomalous procurement patterns, inconsistencies in supplier behavior, and deviations from expected market conditions.

Table 5.1 consolidates heuristic indicators from both research and auditing practice, providing a standardized reference for implementation. Some red flags reflect specific characteristics of the Brazilian institutional and OGD environment, such as social program registries or national sanction lists, yet their underlying risk logic is grounded in patterns identified in the international literature. Although the empirical operationalization is adapted to the Brazilian data ecosystem, the conceptual references in prior studies often address closely related phenomena (e.g., political connections, competition restriction, sanctioned firms, or conflicts of interest), even when derived from different national contexts. Each indicator therefore corresponds to a specific risk hypothesis that can be empirically tested using open datasets, while remaining theoretically anchored in broader research traditions. The inclusion of the “Calculation” and “Limitations” fields acknowledges that red flags do not constitute evidence of fraud but rather probabilistic risk markers subject to contextual interpretation. This hybrid design, grounded in both empirical and expert knowledge, ensures that the model captures not only data patterns but also the auditing rationale behind them, reinforcing interpretability and institutional relevance. While identifying red flags establishes measurable risk indicators, ensuring the traceability of their construction is essential to validating analytical results.

Table 5.1: Risk Indicator Mapping to Data Sources, Calculation Procedures, and Identified Limitations

Code	Source	Indicator	Dataset(s)	Description	Calculation	Limitation
F1	(FAZEKAS; KOCIS, 2020) (VELASCO et al., 2021)	Bolsa Familia Beneficiary Partner	Transparency Portal (Bolsa Familia), CNPJ	Partner receives benefits	CPF-CNPJ match; deduplication	Outdated social data; possible false positives.
F2	(FAZEKAS; KOCIS, 2020) (TISHCHENKO, 2016) Auditor interview	Garantia Safra Beneficiary Partner	Safra Guarantee Program, CNPJ	Partner in the Safra program	CPF-CNPJ match; deduplication	Outdated data; potential inclusion of legitimate beneficiaries.
F3	(NIESSEN; PACIELLO; FERNANDEZ, 2020) (FAZEKAS; TÓTH; KING, 2016) (FAZEKAS; KOCIS, 2020)	Recently Created Company	CNPJ, ComprasNet	New firm before contract	Date diff (open-contract)	Legitimate new firms may appear; context is not considered.
F4	(LISCIANDRA; MILANI; MILLEMACI, 2022) (FAZEKAS; KOCIS, 2020)	Low Share Capital vs. Contract Value	CNPJ, ComprasNet	Low capital-high value	Value ratio (capital-contract)	Share capital may be symbolic; low reliability.
F5	(FERWERDA; DELEANU; UNGER, 2017) (FAZEKAS; KOCIS, 2020) (VELASCO et al., 2021)	Partner with a Political Candidate	TSE, CNPJ	Partner linked to candidate	CPF matches the candidate	Political link does not imply favoritism.
F6	(FAZEKAS; KOCIS, 2020)	Company with Tax Exemptions	Tax Authority, CNPJ	Firm under tax relief	CNPJ match; tax data join	Registry errors may affect classification.
F7	(MARTINEZ-PLUMED et al., 2018) (TISHCHENKO, 2016)	Sanctioned Company	CEIS/CNEP, ComprasNet	Firm previously sanctioned	ID match; sanctions join	Sanctions may be outdated or unrelated.
F8	(TISHCHENKO, 2016) (VELASCO et al., 2021)	Partner as Active Public Servant	Public Servant Registry, CNPJ	Partner is a civil servant	CPF matches the servant list	Some positions lack influence; generalization risk.
F9	(WESTERSKI et al., 2021) (TISHCHENKO, 2016)	Shared Telephone Number	CNPJ	Same phone, multiple firms	Phone std.; duplicate check	Shared contact data may have legitimate reasons.
F10	(WESTERSKI et al., 2021) (TISHCHENKO, 2016)	Shared Email Address	CNPJ	Same email, multiple firms	Email std.; duplicate check	Common emails do not necessarily indicate irregularity.
F11	(WESTERSKI et al., 2021) (BRANDÃO et al., 2024) (FUERTES et al., 2025) (MARTINEZ-PLUMED et al., 2018) (MODRUŠAN; RABUŽIN; MRŠIĆ, 2021)	Shared Business Address	CNPJ	Same address multiple firms	Address std.; geocode; match	Shared locations may be coincidental or legitimate.
F12	(FAZEKAS; TÓTH; KING, 2016) (FERWERDA; DELEANU; UNGER, 2017) (FAZEKAS; WACHS, 2020) (WESTERSKI et al., 2021) (MARTINEZ-PLUMED et al., 2018) (MODRUŠAN; RABUŽIN; MRŠIĆ, 2021)	Partners in Multiple Companies	CNPJ	Partner owns several firms	Partner-firm network link	Legal corporate structures may justify overlap.
F13	(NIESSEN; PACIELLO; FERNANDEZ, 2020) (LISCIANDRA; MILANI; MILLEMACI, 2022) (FAZEKAS; TÓTH; KING, 2016) (FERWERDA; DELEANU; UNGER, 2017) (ULLOA et al., 2025) (FAZEKAS; WACHS, 2020) (DECAROLIS; GIORGIANTONIO, 2022) (TÓTH; HAJDU, 2025) (FAZEKAS; ABDOL, et al., 2022) (GNALDI; DEL SARTO, 2024) (FAZEKAS; TÓTH; ABDOL, et al., 2024) (TÁTRAI; NEMETH, 2018) (OOSTHOEK, 2020) (FUERTES et al., 2025) (MODRUŠAN; RABUŽIN; MRŠIĆ, 2021)	Contracts Obtained Through Bidding	ComprasNet	Contracts via bidding	Classify; ratio (bidding)	Competitive processes may still present risks.
F14	(NIESSEN; PACIELLO; FERNANDEZ, 2020) (LISCIANDRA; MILANI; MILLEMACI, 2022) (FAZEKAS; TÓTH; KING, 2016) (FERWERDA; DELEANU; UNGER, 2017) (ULLOA et al., 2025) (FAZEKAS; WACHS, 2020) (DECAROLIS; GIORGIANTONIO, 2022) (TÓTH; HAJDU, 2025) (FAZEKAS; ABDOL, et al., 2022) (WESTERSKI et al., 2021) (GNALDI; DEL SARTO, 2024) (FAZEKAS; TÓTH; ABDOL, et al., 2024) (TÁTRAI; NEMETH, 2018) (TISHCHENKO, 2016)	Contracts Obtained Without Bidding	ComprasNet	Direct award contracts	Classify; ratio (no bidding)	Legal exemptions are possible; it depends on the contract type.
F15	(FAZEKAS; ABDOL, et al., 2022) (FAZEKAS; TÓTH; ABDOL, et al., 2024) (TISHCHENKO, 2016)	High Contract Value per Capita	ComprasNet, IBGE	High value per citizen	Normalize; join pop; per capita	Regional or budget differences may distort ratios.
F16	(NIESSEN; PACIELLO; FERNANDEZ, 2020) (LISCIANDRA; MILANI; MILLEMACI, 2022) (FAZEKAS; TÓTH; KING, 2016) (ULLOA et al., 2025) (FAZEKAS; ABDOL, et al., 2022) (FAZEKAS; TÓTH; ABDOL, et al., 2024)	High Contract Value Relative to Agency Budget	ComprasNet, Agency Budgets	Value exceeds budget	Normalize; join budget; ratio	The agency budget scale may bias interpretation.
F17	(VELASCO et al., 2021)	Inactive CNPJ	CNPJ	Company registration inactive	Check CNPJ status	Registry inconsistencies may lead to misclassification.
F18	(TISHCHENKO, 2016)	Tax Regime Incompatible with Contract Value	Tax Authority, ComprasNet	Tax type mismatch	Match tax regime; compare	Registration or reporting errors are possible.
F19	(VELASCO et al., 2021)	Company Donations to Political Campaigns	TSE (Donations), CNPJ	Firm donates to campaign	CNPJ match; donation join	Legal donations; no direct fraud evidence.
F20	(MODRUŠAN; RABUŽIN; MRŠIĆ, 2021) (VELASCO et al., 2021)	Partner Donations to Political Campaigns	TSE (Donations), CNPJ	Partner donates to the campaign	CPF match; donation join	Small donations are often irrelevant; low risk.
F21	(MODRUŠAN; RABUŽIN; MRŠIĆ, 2021) (VELASCO et al., 2021)	Partner Affiliation with Political Party	TSE (Party Membership), CNPJ	Partner party member	CPF match; party join	Common membership is not necessarily irregular.
F22	(MODRUŠAN; RABUŽIN; MRŠIĆ, 2021) (VELASCO et al., 2021)	Company Services to Electoral Campaigns	TSE (Campaign Services), ComprasNet	Firm served campaign	CNPJ match; campaign join	Legitimate service provision may occur.
F23	Auditor interview	Ineligible Company (CGU)	CGU Ineligibility List	CGU-ineligible supplier	CNPJ match; CGU join	The record may be outdated or under appeal.
F24	Auditor interview	Ineligible Company (TCU)	TCU Ineligibility List	TCU-ineligible supplier	CNPJ match; TCU join	Possible duplication or outdated sanction.
F25	Auditor interview	Punished Company (CGU)	CGU Sanctions Database	CGU-sanctioned firm	CNPJ match; CGU punishment	Old or unrelated penalties may persist.
F26	(ULLOA et al., 2025) (FUERTES et al., 2025) (MARTINEZ-PLUMED et al., 2018)	CNAE Mismatch with Contract	CNPJ, ComprasNet	Activity not matching contract	CNAE-contract text match	CNAE codes may be generic or misclassified.

Beyond documenting the conceptual origin of each indicator, the table also clarifies the operational pathway through which risk signals are extracted from heterogeneous government datasets. By explicitly linking each red flag to specific data sources and computational procedures, the reference model makes the analytical process transparent and reproducible. This explicit mapping between datasets, calculation logic, and expected limitations allows analysts and auditors to understand not only what signal is being

captured, but also how it emerges from the underlying data infrastructure. In complex public procurement ecosystems, where datasets originate from multiple institutions and vary in structure, coverage, and quality, such transparency is essential to ensure that analytical outputs remain interpretable and methodologically sound.

Additionally, the catalog reveals the multidimensional nature of fraud risk in procurement systems. The indicators collectively capture different types of suspicious patterns, including supplier characteristics (e.g., sanctioned firms or recently created companies), network relationships between individuals and organizations (e.g., shared contacts or ownership structures), political exposure (e.g., donations or affiliations), and anomalies in procurement processes or contract values. By combining these heterogeneous signals, the heuristic layer creates a structured representation of potential vulnerabilities within procurement transactions. These signals subsequently serve as analytical inputs for the subsequent stages of the Engine Layer, where statistical analysis and machine learning models may further explore patterns of irregularity and interaction among indicators.

Table 5.2 presents the distribution of contracts according to the number of red flag indicators identified in the analyzed dataset. For analytical consistency and data reliability, this study focuses on procurement records from 2020 to 2024, resulting in a total of 298,155 contracts extracted from the ComprasNet platform. The yearly distribution of records is as follows: 28,432 in 2020, 37,458 in 2021, 47,522 in 2022, 72,948 in 2023, and 111,795 in 2024. Earlier records available in the platform, particularly those from previous decades, were excluded from the analysis due to noticeable inconsistencies and data quality issues. Within the selected period, the results show that a significant portion of contracts is associated with at least one risk indicator, while progressively smaller proportions exhibit multiple indicators simultaneously. It is important to emphasize that not all red flags defined in the reference model could be computed due to limitations related to data availability, data quality, and integration constraints across the underlying datasets. Nevertheless, even considering only the subset of indicators that could be operationalized, the results provide an informative overview of the incidence of potentially suspicious signals within the analyzed procurement environment. Furthermore, the dataset used in this analysis represents only a subset of the broader ComprasNet ecosystem, restricted to contracts available in the selected period and accessible datasets. Consequently, the observed distribution should be interpreted as an illustrative analytical snapshot rather than a comprehensive measurement of risk across the entire Brazilian public procurement system.

Table 5.2: Distribution of Red Flag Indicators Across Procurement Contracts

Indicators	Quantity	Contracts Flagged	Percentage
1		51646	17.4%
2		20024	6.7%
3		6795	2.3%
4		6551	2.2%
5		1154	0.4%
6		556	0.2%
7		707	0.2%

In addition to the analytical procedures previously discussed, some descriptive indicators derived from the dataset help contextualize the scale and coverage of the analyzed procurement environment. The dataset used in this study contains records associated with 59,595 distinct companies, which represents a very small fraction of the total number of registered companies in Brazil, estimated at approximately 24.9 million. In other words, the supplier universe observed in this dataset corresponds to less than 0.3% of all Brazilian companies, highlighting the selective nature of firms participating in federal procurement processes. From a financial perspective, the contracts contained in the dataset represent an aggregated procurement volume of approximately R\$ 1 trillion between 2020 and 2024, considering only the subset of transactions available through the ComprasNet platform. These figures illustrate the magnitude of the analyzed procurement activity while also reinforcing that the dataset represents only a partial view of the broader Brazilian public procurement ecosystem, as it is restricted to the ComprasNet system and therefore does not encompass the entirety of procurement processes conducted across different governmental levels and platforms.

The analysis also identified a total of 87,433 red flag occurrences across 298,155 contracts within the 2020–2024 period. Figure 5.3 illustrates the temporal evolution of these indicators, showing a consistent increase in the number of detected red flags over time. The number of flagged signals rises from 10,432 in 2020 to 26,232 in 2024, which may reflect both the expansion of available procurement records in recent years and the increasing capacity to operationalize risk indicators within the analytical structure. Beyond

the descriptive statistics presented here, several additional analyses could be conducted to further explore the structure of risk signals in the dataset. Examples include examining the distribution of red flags per contract, identifying the most frequent indicators, analyzing the co-occurrence patterns between different red flags, and exploring clusters of contracts exhibiting similar risk profiles. These possibilities highlight the broader analytical potential of structured procurement data when combined with systematic risk indicators, demonstrating how such datasets can support more advanced forms of fraud risk analysis and decision-support mechanisms for public oversight institutions.

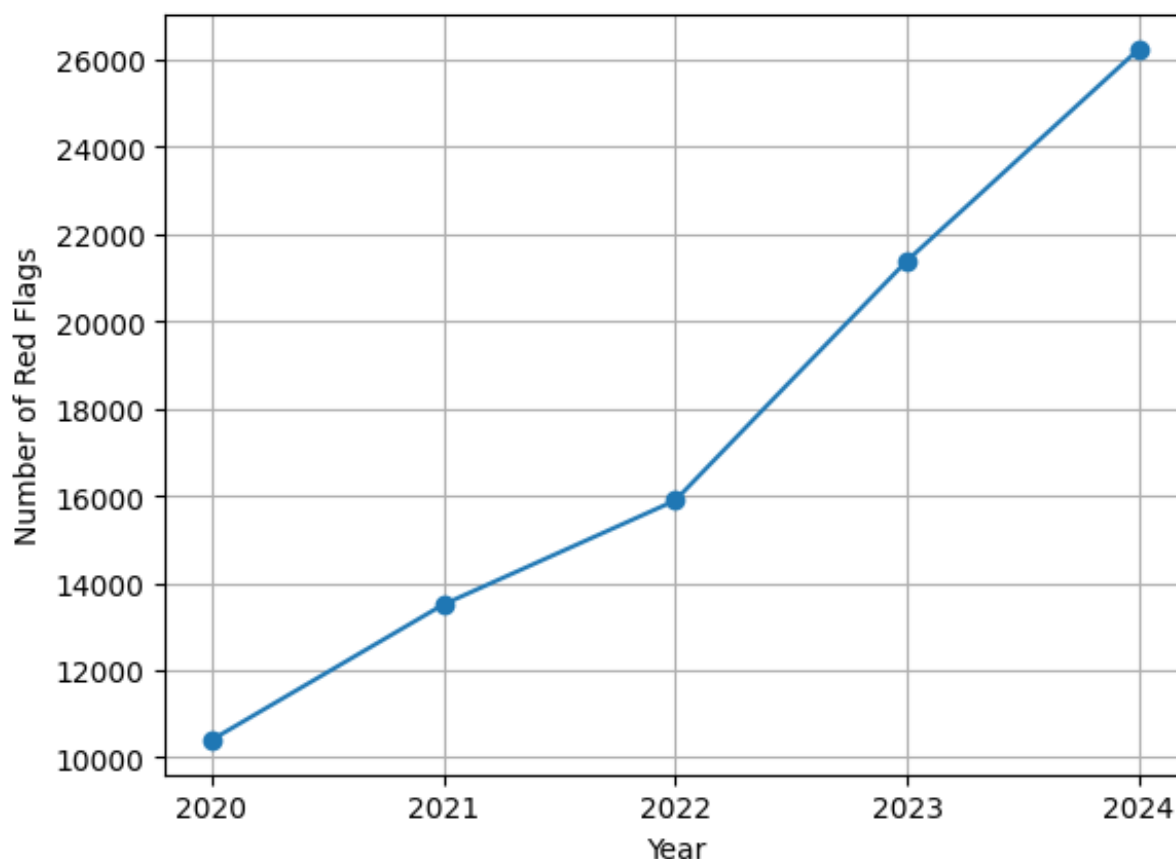


Figure 5.3: Number of Identified Red Flags per Year (2020–2024)

5.2.2 AI Approach

While heuristic indicators and analytical procedures provide interpretable signals of potential irregularities, fraud patterns in public procurement systems may also emerge from complex interactions among multiple variables that are difficult to capture through rule-based logic alone. In this context, the AI approach complements the heuristic layer by enabling the exploration of multivariate patterns and latent structures within the procurement data. Building upon the refined datasets produced in the Data Layer and

the risk indicators derived from the heuristic and analytical procedures, machine learning techniques are employed to support exploratory analysis of procurement behavior. In particular, unsupervised learning methods allow the identification of latent structures within the dataset by grouping contracts according to similarities in selected attributes. Rather than directly classifying contracts as fraudulent, this approach seeks to reveal clusters of procurement transactions that share common structural characteristics and may concentrate higher incidences of risk indicators. In complex procurement environments, where labeled examples of fraud are scarce or incomplete, such exploratory techniques provide an additional analytical perspective that complements rule-based indicators while preserving the interpretability and audit-oriented design of the overall architecture.

Table 5.3 presents the comparative characteristics of the clusters identified through the unsupervised learning procedure using the K-Means algorithm. It is important to note that, due to the exclusion of records containing null values during the preprocessing stage, the total number of observations used in the clustering analysis slightly differs from the dataset size reported previously (298,155), resulting in 295,169 contracts being effectively used in this step.

The results indicate that Cluster 0 concentrates procurement contracts with substantially higher average values, reaching approximately 3.47 million, while Cluster 1 presents a lower average contract value of about 1.53 million. In addition to the difference in financial magnitude, contracts in Cluster 0 also exhibit a higher average number of red flags (0.55) compared to Cluster 1 (0.28), suggesting a greater concentration of potential risk signals within this group. A similar pattern is observed in the distribution of contracts associated with Bolsa Família beneficiaries, with 1,164 occurrences in Cluster 0 against 165 in Cluster 1, reinforcing the presence of stronger risk-related characteristics in the first cluster. Finally, the distribution of contracts across clusters shows that Cluster 0 contains the majority of the procurement records (249,842 contracts), while **Cluster 1 represents a smaller subset of 45,327 contracts, characterized by comparatively lower contract values and fewer associated risk indicators.

Table 5.3: Comparative Characteristics of Procurement Contract Clusters

Feature	Cluster 0	Cluster 1
Average contract value	R\$3.475.272	R\$1.529.865
Average number of red flags	0.55	0.28
Bolsa Familia contracts quantity	1164	165
<u>Total Contracts</u>	<u>249.842</u>	<u>45.327</u>

Another important analytical step in the proposed model involves the use of red flags as a mechanism for generating weak labels that enable the training of supervised machine learning models even in contexts where confirmed fraud labels are not available. In many PP environments, validated cases of fraud are scarce, incomplete, or only identified long after the procurement process has occurred. To address this limitation, the model adopts a weak supervision approach in which each red flag operates as a labeling function that assigns provisional signals of potential risk to procurement contracts. Rather than representing definitive evidence of fraud, these labeling functions capture heuristic indications derived from domain knowledge, regulatory constraints, or patterns previously associated with irregular behavior. By aggregating the outputs of multiple labeling functions, the system is able to construct probabilistic labels that approximate the likelihood of suspicious behavior within the dataset. This mechanism allows the generation of training data for supervised models while maintaining transparency regarding the origin and meaning of each risk signal.

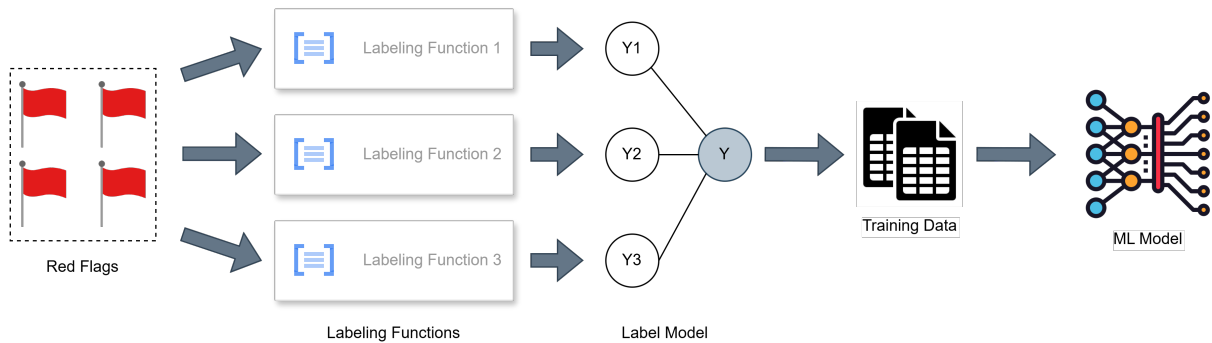


Figure 5.4: Weak Supervised Pipeline

Figure 5.4 illustrates the weak supervision pipeline implemented. In this process, individual red flags operate as labeling functions that analyze procurement records and

independently generate preliminary labels (Y1, Y2, Y3). These outputs represent heuristic signals derived from different risk indicators and domain rules. The signals produced by the multiple labeling functions are then aggregated to produce a consolidated weak label (Y), which serves as the basis for constructing the training dataset. This generated training data is subsequently used to train machine learning models capable of learning patterns associated with suspicious procurement behavior.

The weak supervision approach was implemented using the Snorkel¹³ framework in order to transform the previously defined red flags into labeling functions capable of generating training labels from the procurement dataset. In this process, each red flag operates as a heuristic rule that analyzes specific attributes of a contract and produces a provisional label indicating either potential fraud or non-fraud. When the available information is insufficient to support a decision, the labeling function abstains from assigning a label. By applying this set of labeling functions to the dataset, it becomes possible to generate weak labels even in the absence of manually annotated fraud cases.

The application of the labeling functions was performed over the procurement dataset after the operationalization of the red flags defined in the reference model. Due to limitations related to data availability and integration constraints across the underlying datasets, not all defined red flags could be operationalized as labeling functions. In practice, 17 red flags were successfully implemented and used as labeling functions within the Snorkel framework. Each of these functions independently analyzed specific attributes of the procurement records and generated provisional labels indicating potential fraud, non-fraud, or abstention when insufficient evidence was available. After applying the labeling functions and aggregating their outputs through the weak supervision process, the resulting dataset contained 69,887 contracts provisionally labeled as fraud and 225,282 contracts labeled as non-fraud, totaling 295,169 labeled observations used for subsequent analytical stages. It is important to emphasize that these labels do not represent confirmed fraud cases, but rather probabilistic signals derived from the combination of multiple heuristic indicators. Even so, this process enables the construction of a structured training dataset capable of supporting the development of supervised machine learning models for fraud risk analysis in public procurement environments.

Using the weak labels generated through the labeling functions, a supervised machine learning model was subsequently trained to evaluate the feasibility of learning fraud risk patterns from the constructed dataset. The training process employed the Random Forest

¹³<https://snorkel.readthedocs.io/en/latest/index.html>

algorithm, using a train–test split with a `test_size` of 30%, in which the model was trained on the labeled procurement records and evaluated on the held-out test subset. The resulting performance metrics indicated accuracy, precision, recall, and F1-score values of 100%, suggesting perfect classification performance under the evaluation setting. However, such results should be interpreted with caution. The extremely high performance is likely a consequence of overfitting, meaning that the model may have learned the patterns of the dataset too closely rather than generalizing broader fraud-related behaviors. In addition, because the training labels were generated directly from heuristic labeling functions derived from red flags, the classification task becomes structurally easier for the model, as the same signals used to construct the labels may also appear in the feature space. Therefore, these results should not be interpreted as evidence of a fully reliable fraud detection model, but rather as a demonstration of how weak supervision can generate labeled data that enables the training of machine learning models within the proposed reference model.

Finally, a comparative analysis was conducted between the results obtained through the weak supervision labeling approach and those produced by the unsupervised clustering experiment in order to assess the degree of consistency between the two analytical strategies. Specifically, contracts assigned to Cluster 0 in the clustering analysis—interpreted as the group theoretically associated with lower risk profiles—were compared with the contracts labeled as non-fraud by the labeling functions. The intersection between these two groups resulted in 186,434 contracts out of 249,842, representing 74.6% of the observations in Cluster 0. This substantial overlap suggests a meaningful level of agreement between the two independent analytical approaches. Although clustering and weak supervision rely on different methodological assumptions—one based on unsupervised pattern discovery and the other on heuristic risk indicators—the convergence of results indicates that both methods are capturing similar structural characteristics within the procurement data. Such alignment provides an additional indication that the red flag–based labeling strategy is consistent with broader statistical patterns present in the dataset, reinforcing the analytical coherence of the proposed model for fraud risk analysis in public procurement.

It is important to emphasize that the analyses presented in this section represent only a small subset of the analytical possibilities enabled by the proposed model. The objective of these experiments is not to exhaustively explore all potential analytical strategies, but rather to demonstrate the analytical capacity of the reference model when applied to structured procurement data. Within the proposed architecture, each new analytical

procedure—whether based on statistical analysis, machine learning, clustering techniques, or domain-specific heuristics—can be incorporated as an additional feature or analytical component of the broader system. In this sense, the reference model is conceived as an evolving analytical infrastructure in which new indicators, models, and analytical routines can be progressively integrated over time. Such evolution is expected to occur collaboratively with domain specialists and institutional users of the platform, allowing the analytical capabilities of the system to expand iteratively as new knowledge, data sources, and investigative needs emerge.

5.3 Decision Layer

The Decision Layer translates the analytical outputs generated in the previous layers into practical decision support capabilities for auditors and oversight institutions. In the context of PP oversight, such capabilities are intended to assist investigators in navigating large volumes of procurement data, prioritizing potentially suspicious cases, and exploring the underlying evidence associated with risk indicators. Rather than constituting an automated decision making system, the platform is conceived as an analytical environment designed to support human judgment during auditing and investigative processes.

Given the exploratory and research oriented nature of this work, the Decision Layer was represented through a conceptual prototype developed. In this context, the prototype does not correspond to a fully operational software system, but rather to a composition of analytical components and visualization interfaces assembled to illustrate how auditors could interact with the decision layer in practice. Through simulated dashboards, analytical views, and exploratory visualizations, the prototype demonstrates the potential interaction between users and the analytical outputs produced by the Engine Layer, providing a concrete representation of how the reference model could support fraud risk analysis in real auditing environments.

Figure 5.5 presents a analytical dashboard designed to support the monitoring of procurement risk indicators within the proposed decision support environment. The upper section of the interface displays key summary metrics derived from the analytical pipeline, including the total number of contracts analyzed, the number of cases classified as suspicious using the weak supervision approach (Snorkel), the number of cases flagged through rule based heuristics, and the number of contracts presenting at least one activated red flag. These indicators provide auditors with a high level overview of the dataset and allow

for a rapid assessment of the scale and distribution of potential risk signals identified by the model.

The lower section of the dashboard provides visual summaries of the analytical outputs generated by the Engine Layer. On the left, the Risk Distribution chart illustrates the proportion of contracts categorized into different risk levels based on the combined analytical indicators. On the right, the Most Frequent Red Flags chart highlights the indicators that appear most frequently across the dataset, enabling auditors to identify recurring patterns that may signal procurement vulnerabilities. It is important to emphasize that the values displayed in this interface represent analytical risk signals rather than confirmed cases of fraud. Although the underlying records originate from real procurement data, the classifications produced by the model are intended solely to support investigative prioritization and exploratory analysis by oversight institutions.

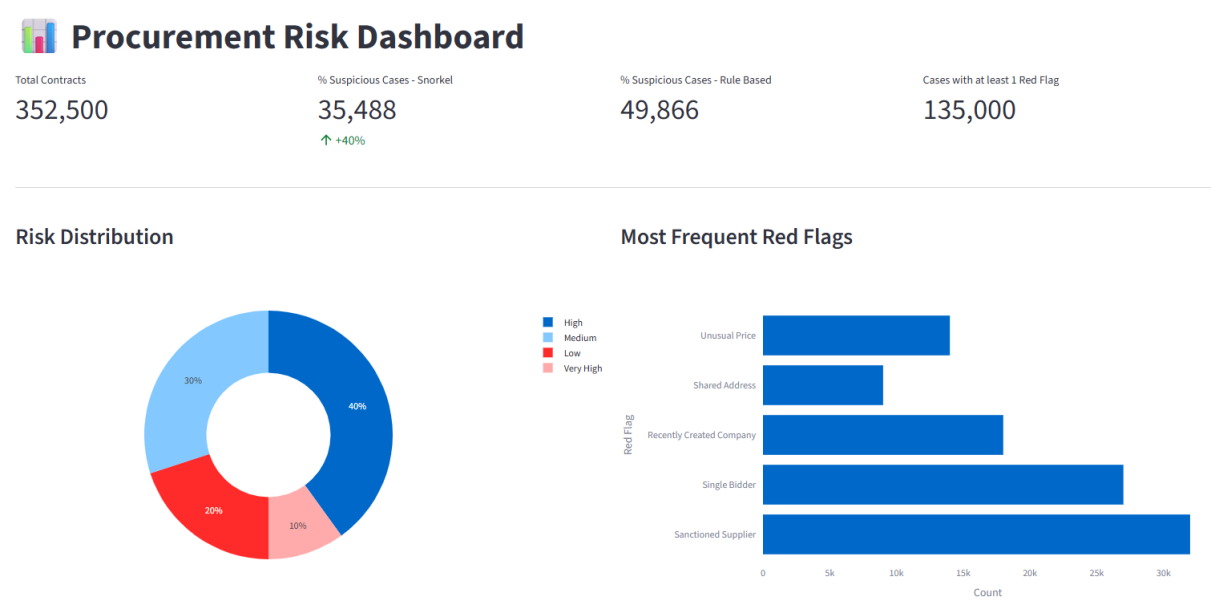


Figure 5.5: Analytical Dashboard for Monitoring Procurement Risk Indicators

Figure 5.6 presents the prototype of the decision-support dashboard designed to support fraud risk monitoring in public procurement. The interface provides auditors with an overview of contracts ranked according to their computed risk score, enabling the rapid identification and prioritization of potentially suspicious cases. On the left side of the dashboard, the system displays a table of Top Risk Contracts, listing procurement records alongside key attributes such as contract identifier, supplier, associated public agency, number of activated red flags, and a normalized risk score that reflects the aggregation of analytical signals generated by the Engine Layer. This ranking mechanism allows oversight professionals to quickly focus their attention on contracts that exhibit

higher levels of anomalous behavior according to the analytical model.

The right panel presents the Activated Red Flags associated with the contract currently selected by the user, summarizing contextual information such as the supplier, contracting authority, overall risk score, and the number of triggered indicators, while also listing the specific risk signals responsible for the elevated risk classification (e.g., supplier appearing in sanction registries, shared contact information between companies, or recently created firms participating in procurement procedures). By explicitly exposing the activated indicators, the dashboard provides interpretable explanations for the analytical results and supports transparency in the decision support process. In this way, the interface functions as an initial triage mechanism, allowing auditors to identify contracts that require further attention before proceeding to a subsequent investigation interface, where the full set of contract attributes can be examined in detail and the case can be formally assessed through classification options and expert annotations.

Procurement Risk Dashboard

Decision support prototype for public procurement fraud risk analysis

Top Risk Contracts

Contract ID	Supplier	Risk Score	Red Flags	Agency
15304899008082023	P H MENESES COMERCIO LTDA	0.89	3	UNIVERSIDADE FEDERAL DO ES
07001999006652023	P H MENESES COMERCIO LTDA	0.84	2	JUSTICA ELEITORAL
25004299011702024	APR COMERCIO DE CORRELATOS PARA SAUDE LTDA	0.81	4	MINISTERIO DA SAUDE
16005850000022023	BARUC SERVICOS E REPRESENTACOES LTDA	0.77	2	COMANDO DO EXERCITO
25444850000022022	PERKINELMER DO BRASIL ANALITICA LTDA	0.74	1	FUNDACAO OSWALDO CRUZ

Activated Red Flags

Select a contract

15304899008082023

Contract ID: 15304899008082023
 Supplier: P H MENESES COMERCIO LTDA
 Agency: UNIVERSIDADE FEDERAL DO ESPIRITO SANTO
 Risk Score: 0.89
 Number of Red Flags: 3

Activated indicators:

- Supplier in sanction registry
- Shared phone number with another supplier
- Recently created company

Figure 5.6: Procurement Risk Dashboard for Monitoring Contracts and Activated Red Flags

Figures 5.7, 5.8, 5.9 and 5.10 illustrate the detailed contract level investigation interface of the proposed decision support system. After a contract is selected in the risk monitoring dashboard, the system opens a comprehensive analytical view that consolidates all relevant information associated with the procurement case. The interface presents a structured overview including contract metadata, procurement process characteristics, supplier information, participating bidders, activated red flags, and analytical explanations describing the contribution of different factors to the computed risk score. In addition, the interface provides access to supporting documentation such as the tender notice and contract documents, as well as the provenance of the datasets used in the analysis. This integrated view is designed to support auditors during the investigative stage by

enabling a deeper examination of the contextual, organizational, and analytical aspects of each contract. At the end of the interface, auditors can formally assess the case by classifying it as evidence, inconclusive, or monitoring, and record qualitative observations through textual comments. This functionality allows the system to support not only automated risk identification but also structured human judgment and case documentation during the audit process.

Procurement Case Analysis

Detailed contract-level investigation interface for fraud risk analysis in public procurement

Contract ID	Risk Score	Red Flags	Risk Level
1530489900082023	0.89	3	HIGH

Contract Summary

Procurement Process: 2023/000145	Contract Value: R\$ 4,580,000
Procurement Object: Medical laboratory equipment acquisition	Estimated Value: R\$ 4,600,000
Contracting Agency: Universidade Federal do Espírito Santo	Price Difference: -0.4%
Procurement Modality: Pregão Eletrônico	
Contract Date: 12/05/2023	
Contract Duration: 12 months	
Open Tender Notice (PDF)	Open Contract Document
	Open Procurement Portal

Figure 5.7: Case Overview and Risk Indicators

Supplier Information	Procurement Details						
Supplier Name: P H Meneses Comercio Ltda	Number of Bidders: 2						
CNPJ: 12.483.029/0001-88	Bid Submission Period: 3 days						
Company Age: 2 years	Average Market Bidders: 7						
Headquarters: Vitória - ES	Competing Suppliers:						
Economic Activity (CNAE): Medical equipment trade	<table><tr><th>Supplier</th><th>Status</th></tr><tr><td>PH Meneses Comercio Ltda</td><td>Winner</td></tr><tr><td>Baruc Serviços e Representações Ltda</td><td>Competing bidder</td></tr></table>	Supplier	Status	PH Meneses Comercio Ltda	Winner	Baruc Serviços e Representações Ltda	Competing bidder
Supplier	Status						
PH Meneses Comercio Ltda	Winner						
Baruc Serviços e Representações Ltda	Competing bidder						
Sanctions Registry: YES (1 record found)							
Previous Government Contracts: 14							
Historical Contract Value: R\$ 22,300,000							
Related Companies Identified:							
- Meneses Distribuidora Ltda - PHM Comercial							
Shared Contacts Identified:							
- Phone: (27) 3333-2244 - Email domain overlap detected							

Figure 5.8: Activated Red Flags and Analytical Explanations

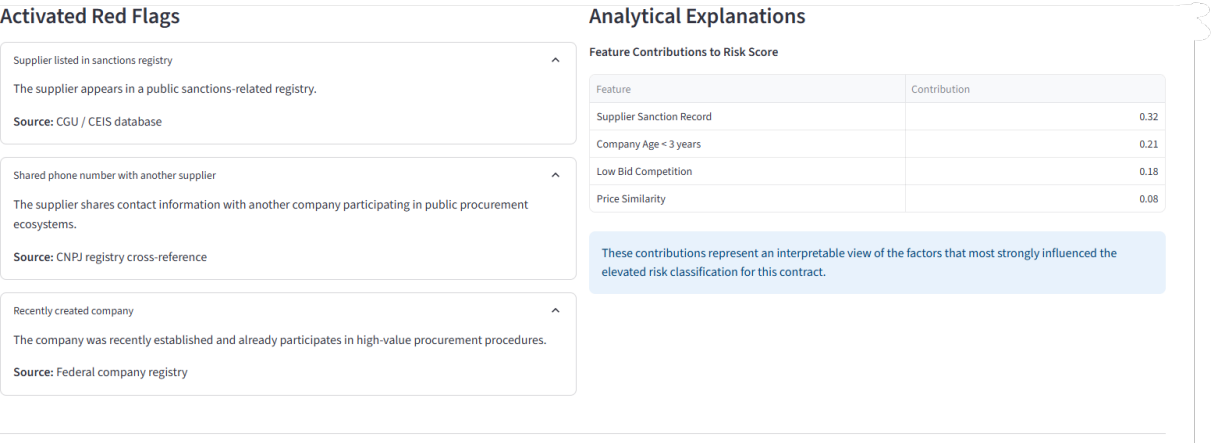


Figure 5.9: Supplier Information and Procurement Details

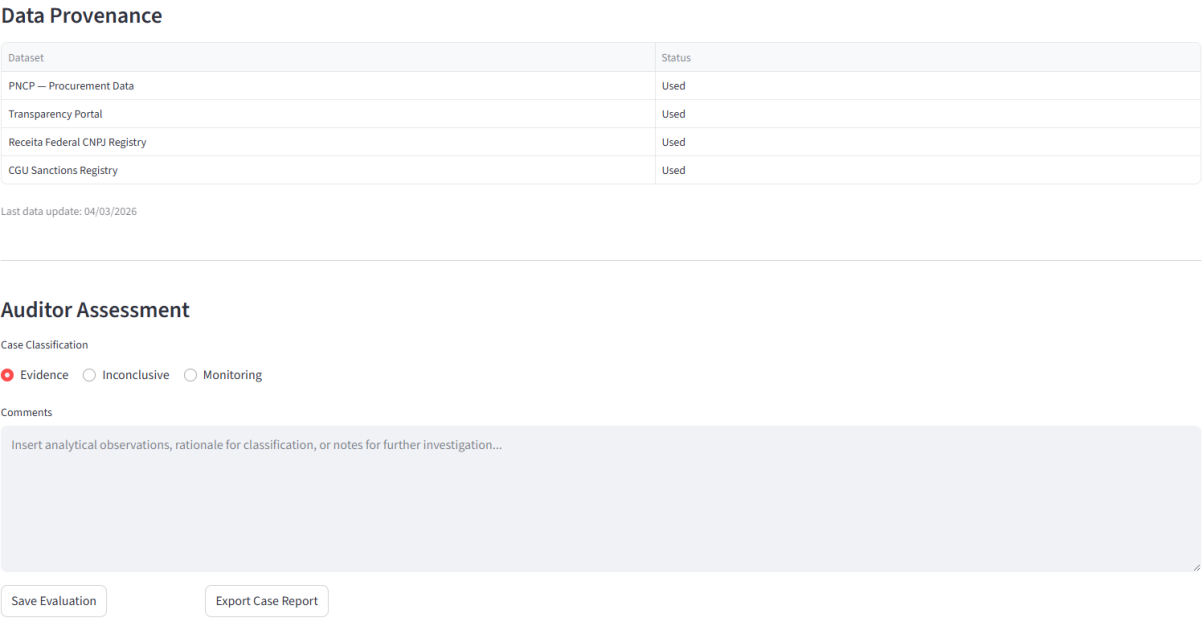


Figure 5.10: Data Provenance and Auditor Assessment

It is important to emphasize that the contracts displayed in the prototype correspond to real procurement records obtained from public datasets, but the risk classifications presented in the interface do not represent confirmed cases of fraud or corruption. Instead, they reflect analytical signals generated by the model, which identify patterns that may warrant further investigation by oversight authorities. In this sense, the dashboard should be interpreted as a decision support environment designed to assist auditors in prioritizing cases and exploring potential irregularities, rather than as an automated mechanism for determining fraudulent behavior.

If the auditor wishes to analyze the dataset as a whole, performing searches, cross-referencing information, or exploring procurement records beyond individual cases, this

can be done through the interface illustrated in the Figure 5.11. This screen provides an exploratory environment where users can interact with the underlying data through a graphical interface, enabling filtering, sorting, and navigation across procurement records and related entities. Additionally, the interface allows more advanced users to directly query the data using SQL, enabling the execution of customized analytical queries and more complex data investigations. This functionality supports deeper exploratory analysis and facilitates flexible interaction with the dataset, complementing the contract-level investigation tools provided by the system.

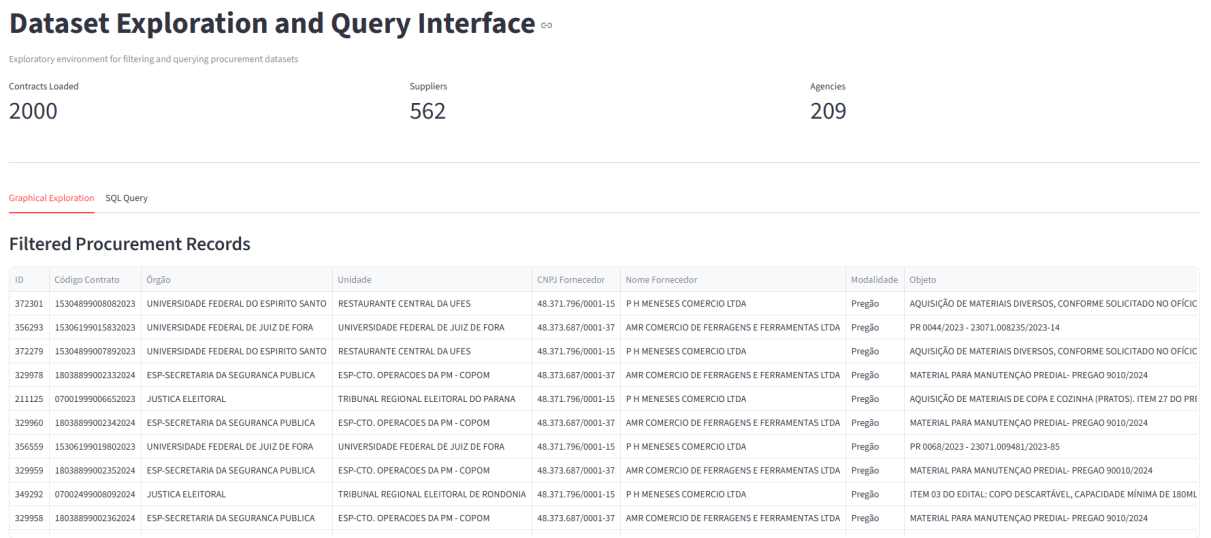


Figure 5.11: Dataset Exploration and Query Interface

5.4 Ethical Layer

The Ethical Layer constitutes a cross cutting dimension of the proposed reference model, permeating all other layers of the architecture. The application of AI and data driven analytics in public sector auditing introduces significant institutional and societal implications, as analytical outputs may influence investigative priorities and potentially affect the reputation and economic standing of companies involved in PP processes. For this reason, the design and deployment of such systems must incorporate mechanisms that promote responsible and trustworthy use of data and algorithms. In this context, ethical considerations are operationalized through principles such as transparency, explainability, auditability, data provenance, and human oversight, ensuring that both the analytical processes and the underlying data transformations can be traced, verified, and critically evaluated by human auditors. By embedding these ethical principles into the architecture itself, the system seeks to support data driven decision making while preserving institu-

tional accountability and safeguarding against unintended harms arising from automated or semi-automated analytical processes.

5.4.1 Human Oversight and Accountability

The interaction between the auditor and the analytical platform is implemented and illustrated in Figure 5.12. In this process, the platform receives both automated inputs derived from data processing mechanisms and direct interactions from the auditor through the system interface. The automated inputs originate from the integration of datasets and the execution of analytical algorithms and processes responsible for generating indicators, patterns, and risk signals related to public procurement activities. These computational components transform raw data into analytical outputs that are presented to the auditor within the platform.

However, the final analytical interpretation and decision-making process remains under the responsibility of the auditor. As shown in the figure, the auditor evaluates the outputs generated by the system based on multiple sources of contextual knowledge, including regulations and legal frameworks, accumulated audit knowledge, and empirical or practical information derived from professional experience. In the implemented environment, the auditor may take actions within the platform, such as classifying cases, providing comments, or initiating further investigative procedures. This interaction establishes a human in the loop analytical process in which automated analytical capabilities support, but do not replace, human judgment and institutional accountability in public sector auditing.

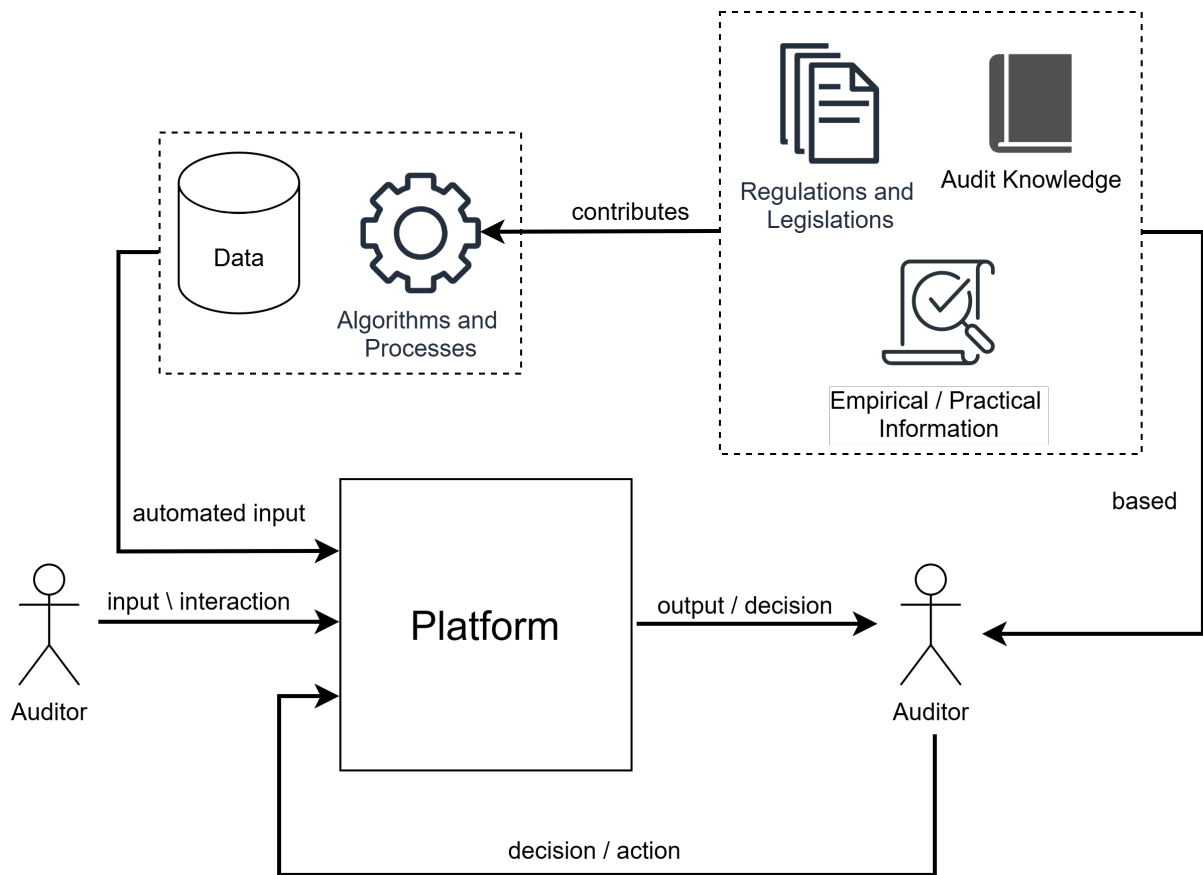


Figure 5.12: Human in the Loop Analytical Process in the Procurement Risk Analysis Platform. Adapted from (KYRIAKOU; OTTERBACHER, 2023)

5.4.2 Transparency, Explainability and Provenance

The principles of transparency, explainability, and provenance constitute fundamental mechanisms for ensuring the responsible use of AI supported analytical systems in public sector contexts. In environments such as PP auditing, analytical outputs may influence investigative priorities and potentially affect the reputation of companies or institutions involved in procurement processes. For this reason, it is essential that the analytical processes performed by the system remain traceable, transparent and understandable.

In order to increase the interpretability of the analytical models implemented in the platform, explainable artificial intelligence (XAI) techniques were incorporated into the instantiated system. These techniques allow auditors to understand how different variables contribute to the predictions generated by the fraud risk detection models. In the context of PP auditing, such interpretability is particularly important, as algorithmic outputs may influence investigative priorities and potentially affect the evaluation of procurement processes. Following the approach presented in the study reported in (SAMPALIO; FONTES,

et al., 2024), explainability techniques were applied to the predictive models used in the platform in order to provide both global and local explanations of model behavior.

The instantiated platform incorporates a provenance mechanism designed to record the relationships between data entities, computational processes, and system components involved in the analytical workflow. In the implemented environment, provenance information is captured during the execution of data ingestion, transformation, and analytical procedures responsible for generating procurement records and fraud risk indicators. This mechanism allows the system to maintain a structured record of how analytical outputs are derived from the underlying datasets used in the fraud risk analysis process, enabling the traceability of data transformations and analytical operations throughout the platform, which is a key requirement for ensuring transparency and accountability in data-driven systems (MORA-CANTALLOPS et al., 2021).

Figure 5.13 illustrates how these provenance relationships are represented within the platform. The diagram shows how procurement related data entities, such as supplier records, procurement transactions, and red flag indicators, are connected through activities that represent the analytical operations performed by the system. Each activity records temporal and contextual information regarding the processes that generated or transformed the data. By capturing these relationships, the implemented provenance structure allows auditors to trace how specific analytical outputs were produced, supporting traceability, auditability, and transparency within the fraud risk analysis environment.

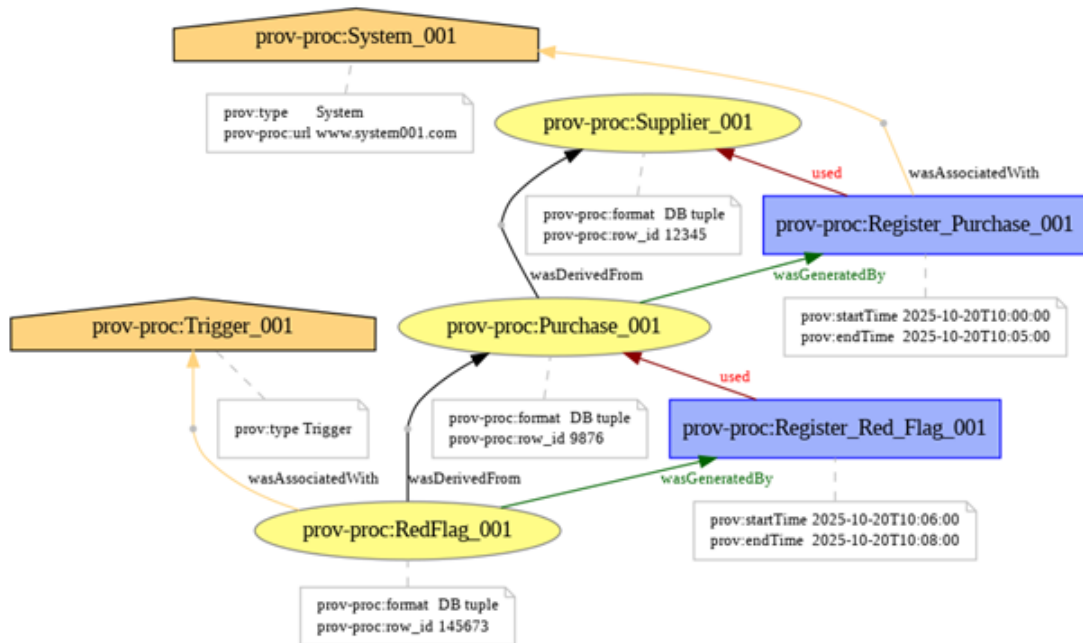


Figure 5.13: Provenance Representation of Data Transformations and Indicators Generation in the Implemented Analytical Platform

5.5 Governance and Security Layer

The Governance and Security Layer constitutes a cross cutting component of the proposed reference model, designed to ensure that the processes of data integration, risk indicator generation, and analytical decision support operate within appropriate standards of transparency, accountability, and data protection. Given that fraud risk analysis in PP involves the processing of large volumes of administrative data and potentially sensitive information, this layer establishes mechanisms that regulate how data is accessed, processed, and interpreted within the system. In the instantiation developed in this research, these governance and security considerations are embedded directly into the system architecture through features such as controlled data access, traceability of analytical outputs, and structured management of risk indicators and supporting evidence.

The system implements a comprehensive logging mechanism in which every interaction performed by a user is automatically recorded. This includes events such as user authentication, navigation between system modules, selection of contracts, inspection of analytical indicators, button clicks, submission of case assessments, etc. The objective of this mechanism is to ensure full traceability of the analytical process, enabling both the analysis of auditor interaction patterns within the system and the preservation of a verifiable record of all actions performed during the investigation. This record can serve as evidence in future reviews or audits of the auditor's analytical work, ensuring accountability and transparency in the decision making process.

Table 5.4 illustrates an example of the structured logs generated by the system. Each record contains a Timestamp, indicating the exact moment at which the interaction occurred, and a User field identifying the authenticated user responsible for the action. The Log Type column categorizes the type of event performed (e.g., login, contract selection, analysis action), while the Source column indicates the system module or interface where the interaction took place. In addition, the IP Address and MAC Address fields store network-level identifiers associated with the user session, supporting security auditing and traceability of system access. Finally, the Interaction Log (JSON) column points to a detailed JSON file stored on the server that contains the full interaction trace, including fine-grained behavioral information such as the exact text typed by the user, keystroke sequences, mouse clicks, navigation patterns, inactivity periods, and other contextual metadata. This architecture enables the reconstruction of user interactions with the system and supports governance, accountability, and forensic analysis of analytical workflows within the decision-support environment.

Table 5.4: System Interaction Logging Structure for Audit Traceability

Timestamp	User	Log Type	Log Module	Source	IP Address	MAC Address	JSON File Index
2026-03-01 12:00:52	auditor1@email.com	Comment Submission	Auditor Assessment Module	/case_inspection	192.168.0.26	00:1A:2B:4C:4D:5E	99baec504a1fe91a07bc66b6900bd3987419188.json
2026-03-01 12:01:52	auditor2@email.com	Dataset Access	Procurement Dashboard	/main_dashboard	192.168.0.24	00:1A:2B:5C:4D:5E	57168339c7c2a8eb408790afaff6e0ec8b62ed89.json
2026-03-01 13:02:52	auditor3@email.com	Contract Selection	Risk Dashboard	/risk_dashboard	192.168.0.23	00:1A:2B:6C:4D:5E	86f7e437faa5a7fce15d1ddcb9eaeaea377667b8.json
2026-03-01 13:02:58	auditor4@email.com	Case Classification	Auditor Assessment Module	/case_inspection	192.168.0.22	00:3A:2B:3C:4D:5E	dfa54516f02d5b2e59238643bdfed0d9831e87447.json
2026-03-01 13:05:01	auditor5@email.com	Login	Authentication Module	/login	192.168.0.21	00:1A:2B:3C:4D:5E	042dc4512fa3d391c5170cf3aa61e6a63f84342.json

The system also implements a role-based access control mechanism in which users are assigned to different access groups, each with distinct permissions regarding the functionalities and data available within the platform. This approach ensures that sensitive information and critical system operations are accessible only to authorized users, reinforcing governance and security practices within the analytical environment, as illustrated in Figure 5.14. For example, administrator users have full access to the system, including user management, configuration of datasets, and access to system logs and governance-related information. Auditor users are granted access to the core analytical functionalities, such as dataset exploration, contract inspection interfaces, red flag analysis, and the ability to classify cases and provide comments or assessments. In contrast, viewer or observer users have more restricted permissions, typically limited to consulting dashboards, aggregated indicators, and predefined reports without the ability to modify classifications or interact with case assessment modules. This layered access structure allows the system to support different institutional roles, such as auditors, analysts, and system administrators, while maintaining appropriate levels of control, accountability, and protection of sensitive analytical processes.

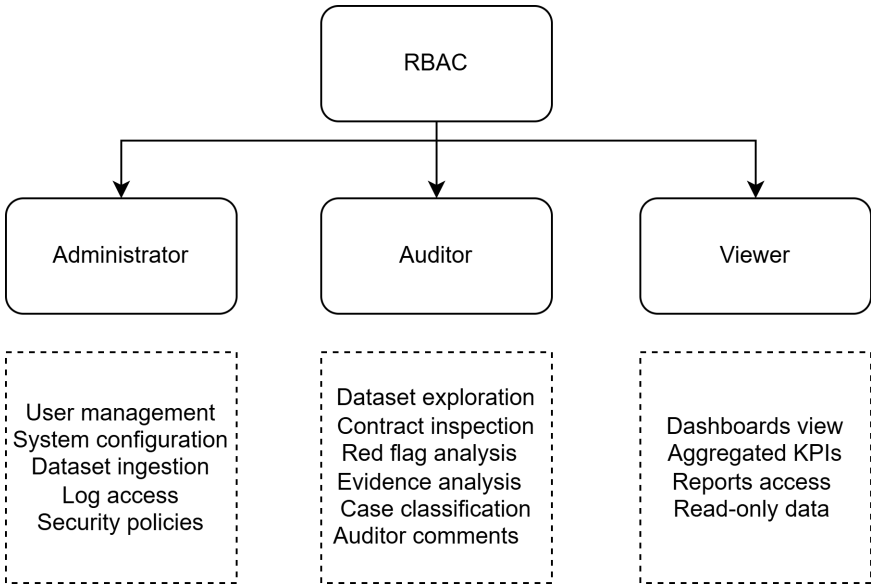


Figure 5.14: RBAC Structure

5.6 Discussion and Limitations of the Reference Model Instantiation

Although the proposed reference model provides a structured based fraud risk analysis in PP, not all of its components could be fully instantiated within the scope of this research. One important limitation relates to the temporal and practical constraints inherent to a doctoral research project. Several elements of the model, such as the development of a fully operational system, the implementation of complete data pipelines, and the longitudinal evaluation of analytical outputs, would require longer development cycles and sustained institutional collaboration. Consequently, the instantiation presented in this work focuses primarily on demonstrating the feasibility of the core analytical components of the model, particularly the generation of fraud risk indicators and their integration into a decision support environment.

A second limitation concerns the dependence on institutional integration for the implementation of certain components of the model. Some functionalities would require direct interaction with governmental systems or oversight bodies, such as integration with internal audit platforms, access to restricted databases, or the operational use of the system by auditors within real oversight environments. These forms of integration were beyond the operational scope of this research and would require formal institutional partnerships and governance arrangements that extend beyond the boundaries of an academic research project.

In addition, the availability and quality of datasets impose practical constraints on the instantiation of several analytical components. Although OGD initiatives provide an increasingly important source of information for research and transparency, the datasets available are not always complete, standardized, or easily integrable. This limitation is common in many open data ecosystems and affects the extent to which certain indicators or analytical procedures can be operationalized using publicly accessible information alone.

Finally, it is important to emphasize that the objective of this research is the development of a reference model, rather than the implementation of a fully operational production system. By definition, reference models function as conceptual and architectural blueprints that guide the design and implementation of systems within a given domain. In this sense, the value of the proposed model lies in structuring the key components, data flows, and analytical mechanisms required for fraud risk analysis in public

procurement, while providing a foundation that can be extended, adapted, and operationalized in future implementations carried out by governmental institutions or research initiatives.

Chapter 6

Results and Evaluation

The development of artifacts within the DSR paradigm requires not only the formulation of a theoretically grounded solution, but also a structured examination of its empirical behavior and institutional adequacy. In this research, the referenced model was conceived as a sociotechnical decision-support artifact designed to support fraud risk analysis in PP through the integration of open government data, red flags, provenance mechanisms, and analytical components. Consequently, the systematic presentation and evaluation of results constitute a fundamental step to demonstrate the model’s relevance, interpretability, and alignment with oversight practices.

This chapter presents the empirical results generated by the execution of the referenced model and reports the findings of three complementary expert-based evaluation studies conducted with public auditors. First, the chapter clarifies the adopted evaluation strategy and the conceptual meaning of evaluation within this thesis. Second, it presents the results of three structured studies: (i) the assessment of data sources and risk indicators for fraud detection in public procurement, (ii) the technical evaluation of PP cases with potential fraud indicators, and (iii) the evaluation of ethical aspects in AI-based fraud detection. Finally, the chapter integrates these findings, discussing their design implications and outlining the limitations of the current evaluation scope.

6.1 Evaluation Strategy

Within the DSR paradigm, evaluation is not conceived as a post hoc measurement of technical performance alone, but as a reflective process that examines the adequacy and implications of design decisions throughout the artifact’s lifecycle. Rather than focusing exclusively on benchmarking predictive metrics, the evaluation strategy adopted in this

thesis seeks to determine whether the referenced model fulfills its intended role as a decision-support instrument in public procurement oversight. Evaluation is therefore understood as a mechanism for critically examining the model's structural coherence, interpretability, institutional plausibility, and ethical alignment within its operational context.

In the specific context of this research, evaluation refers to the structured assessment of key design constructs that underpin the referenced model, rather than to the exhaustive validation of predictive accuracy across all possible procurement scenarios. The evaluation focuses on three interrelated dimensions that reflect the conceptual architecture of the model. First, the adequacy and relevance of selected data sources were examined to determine whether the adopted public procurement portals and open datasets provide a meaningful foundation for fraud risk analysis. Second, the plausibility and interpretability of the proposed red flags were assessed, considering their capacity to translate heterogeneous procurement data into analytically coherent and operationally understandable risk signals. Third, ethical considerations embedded in the model were examined, particularly those related to transparency, accountability, and responsible use in public-sector decision-making. Together, these dimensions form a coherent evaluative triad that mirrors the socio-technical structure of the referenced model.

The evaluation was operationalized through three structured studies conducted with public-sector auditors from federal, state, and municipal levels. These studies were designed to examine the referenced model from an institutional perspective, drawing upon the professional experience of domain experts engaged in procurement oversight. Rather than treating auditors as passive respondents, the studies sought to capture informed judgments regarding the adequacy of data sources, the technical plausibility of risk indicators when applied to concrete cases, and the ethical implications associated with AI-supported fraud detection. This approach situates evaluation within a socio-technical framework, recognizing that the legitimacy and practical applicability of analytical tools in public procurement depend not only on internal analytical logic but also on their coherence with institutional norms and professional judgment.

6.2 Expert-based Evaluation

The expert based evaluation was conducted through structured questionnaires administered to public auditors from federal, state, and municipal levels of government. The

instrument combined multiple-choice questions and open-ended prompts, allowing both structured assessment and qualitative insights. All evaluative items were measured using Likert-scale questions to capture degrees of agreement regarding data source adequacy, red flag interpretability, and ethical alignment. In addition, each question included a free-comment field, enabling auditors to elaborate on their responses and provide contextual reflections based on their professional experience. To ensure confidentiality and mitigate any risk of institutional or professional exposure, no identifying information was collected from participants. This anonymity was considered essential to promote candid responses and safeguard auditors against potential reputational or organizational repercussions.

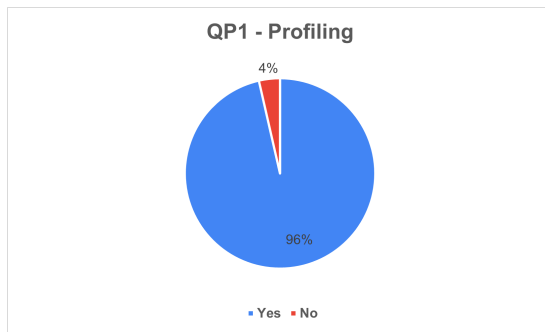
6.2.1 Data sources and risk indicators

This subsection presents the results of the expert based evaluation concerning the adequacy and relevance of the data sources integrated into the referenced model. The assessment was conducted with 28 experienced public auditors through a structured questionnaire designed to examine whether the selected public procurement portals and open government datasets constitute a meaningful and reliable foundation for fraud risk analysis. The objective was to evaluate whether the adopted data collections are technically suitable and operationally aligned with the informational needs of public procurement oversight and control.

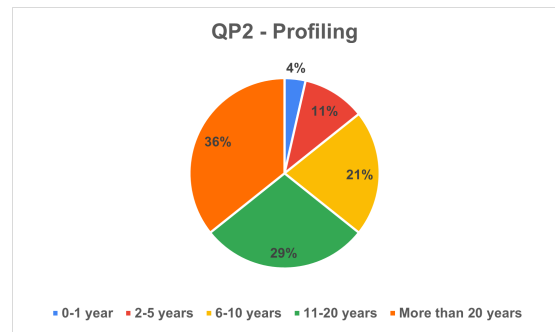
Auditors were invited to assess the relevance, completeness, and practical applicability of the datasets used to construct the risk indicators. Using Likert-scale questions complemented by open-ended comment fields, participants provided their professional judgments regarding the adequacy of the data sources for detecting irregularities and supporting investigative processes. The qualitative feedback offered insights into perceived limitations, potential data gaps, and suggestions for refinement, contributing to a more context-sensitive understanding of how the data infrastructure of the referenced model aligns with the operational realities of public-sector auditing in Brazil.

The questionnaire began with questions aimed at understanding the profile of the participants and their experience in the auditing area. The first question (Q1) investigated whether the respondents worked directly in auditing or controlling, allowing us to identify the practical relevance of their answers in the study context. Next, the auditors were asked (Q2) about their sphere of activity — municipal, state, federal, or other — allowing us to map the scope of the feedback collected. The third question (Q3) sought to understand the participants' experience by asking how many years they had been in the auditing

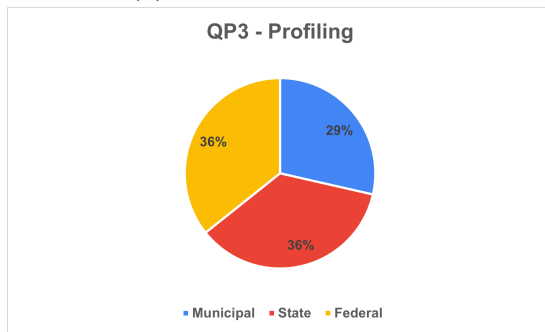
area, categorizing them into levels of seniority. Finally (Q4), the questionnaire explored the degree of contact of the auditors with fraud in PP, ensuring that the analysis of red flags considered the perspective of professionals familiar with irregular practices. The results of these questions can be seen in Figure 6.1, and the translation of the questions and answers can be seen in Table 6.1. Considering that the questionnaire was addressed to Brazilians, all the answers collected were initially given in Portuguese, so each figure representing one or more answers will be accompanied by a translation table into English.



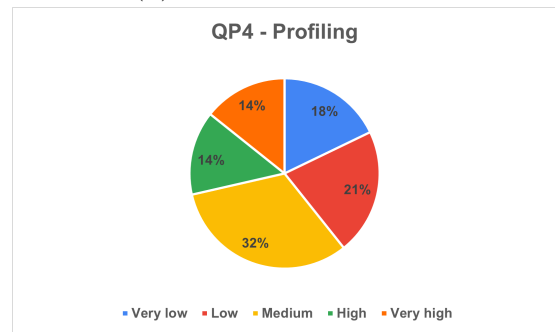
(a) Question Profiling 1



(b) Question Profiling 2



(c) Question Profiling 3



(d) Question Profiling 4

Figure 6.1: Answers to profiling questions

Table 6.1: Profiling Questions

Question	Translated Question Text	Translated Alternatives
QP1	Do you work in auditing or controlling?	Yes No
QP2	In what sphere of activity do you perform your role?	Municipal State Federal
QP3	How many years of experience do you have in auditing?	0-1 year 2-5 years 6-10 years 11-20 years Over 20 years
QP4	What is your degree of contact with fraud in public procurement?	Very low Low Medium High Very high

The second section of the questionnaire focused on assessing the relevance of various datasets in the context of fraud detection. Participants were presented with a list of public datasets. For each dataset, respondents were asked whether they considered it relevant for detecting fraud, with an optional follow-up question allowing them to justify their answers. At the end of this section, a final open-ended question invited participants to suggest any additional public datasets they deemed relevant for the study. This structure provided valuable insights into the practical applicability of existing datasets and potential gaps in the resources available for fraud detection. Each question about the relevance of a specific dataset included three response options: "Yes," "No," and "I do not know or prefer not to answer." This structure allowed participants to express their agreement or disagreement with the dataset's applicability while providing an option for uncertainty or reservation, ensuring inclusive and comprehensive feedback.

The results of the subsequent questions in this section are presented in Figure 6.2, which summarizes the responses for each dataset. The exact wording of the questions and their corresponding response options can be found in Table 6.2 for reference.

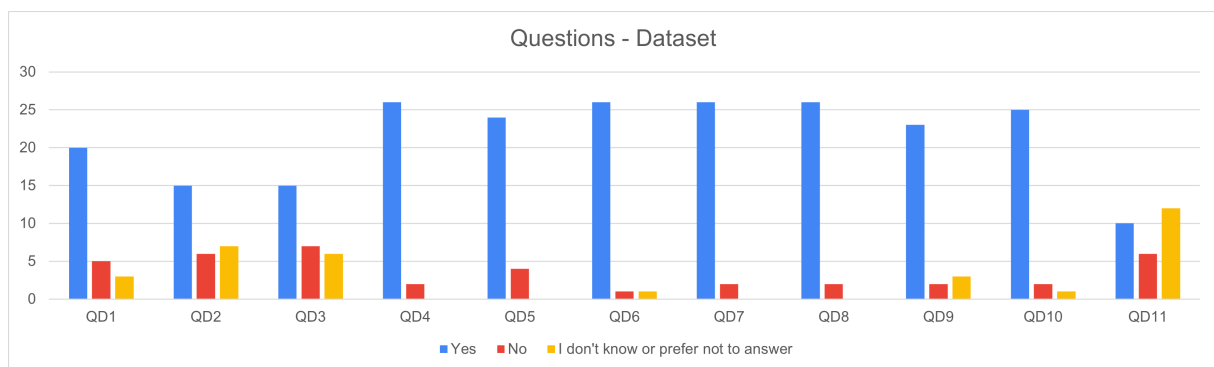


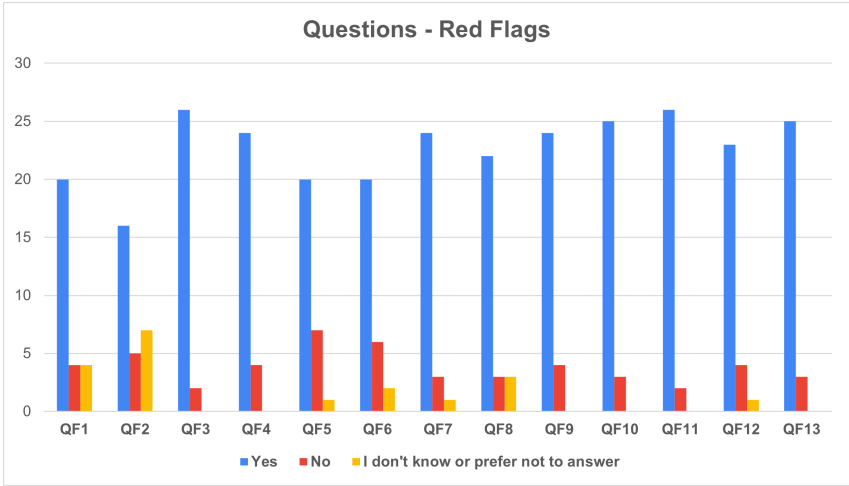
Figure 6.2: Answers to datasets questions

Table 6.2: Datasets Questions

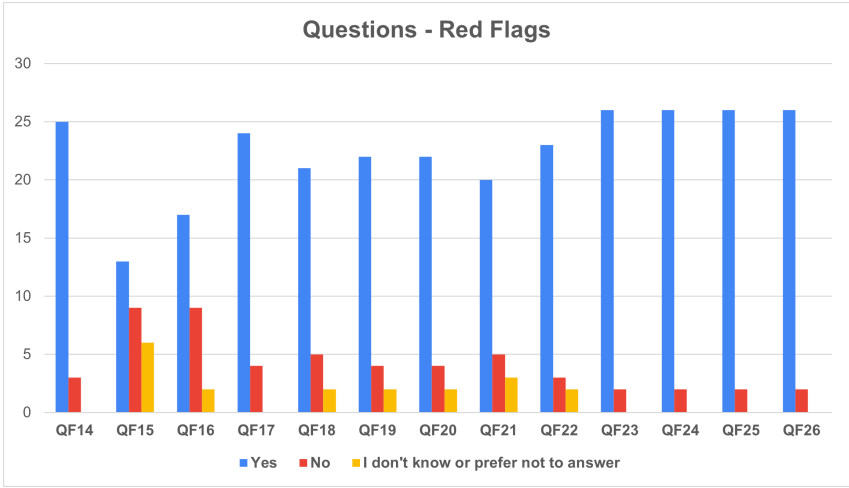
Question	Translated Question Text
QD1	Bolsa Família - Payments
QD2	TSE
QD3	CATMAT/CATSER
QD4	Contracts (GOV BR Contracts)
QD5	Companies (CNPJ Registration)
QD6	Unreliable Companies
QD7	Unreliable and Suspended Companies
QD8	Punished Companies
QD9	Suppliers
QD10	Invoices
QD11	Safra Guarantee

The third section of the questionnaire was designed to validate the red flags proposed in the study directly. Auditors were asked to assess each red flag's practical relevance in detecting fraud in PP. This step sought to capture insights into the applicability of the indicators in day-to-day audits and identify possible gaps or adjustments needed to improve the indicators presented. By adopting a practical approach, this section also explored auditors' perception of the ability of red flags to reflect patterns and behaviors typical of fraudulent practices, providing a solid basis for contextualizing and refining the metrics used in the study.

The results of the subsequent questions in this section are presented in Figure 6.3, which summarizes the responses for each dataset. The exact wording of the questions and their corresponding response options can be found in Table 6.3 for reference.



(a) Red Flags Questions 1-13



(b) Red Flags Questions 14-26

Figure 6.3: Answers to red flags questions

Question	Red Flag Indication	Description
FQ1	Bolsa Família Beneficiary Member	Check if any of the company's partner members and/or the person responsible for the supplier has any connection with the Bolsa Família Social Program
FQ2	Garantia Safra Beneficiary Member	Check if any of the company's partner members have any connection with the Garantia Safra Social Program
FQ3	Company Opening Date	Check the difference between the company's opening date and the contract signing date
FQ4	Company Share Capital	Check the difference between the company's share capital and the contract value
FQ5	Political Member/Candidate	Check if any of the partner members is or has been a candidate for any political office
FQ6	Company Tax Exemption	Check if the company has any tax exemption
FQ7	Company Sanctions Against	Check if the company has any sanctions by the Government
FQ8	Active Public Servant Member	Check if any of the partner members is a public servant
FQ9	Company Telephone	Check if the company has the same telephone number as another company(ies)
FQ10	Company Email	Check if the company has the same email as another company(ies)
FQ11	Addresses Related to the Company	Check if the company has its headquarters at the same address as another company(ies)
FQ12	Company Partners	Check if the partners are partners in other companies
FQ13	Contracts With Bidding	Check the percentage of contracts won through bidding
FQ14	Contracts Without Bidding	Check the percentage of contracts won without bidding
FQ15	Contract Value per 100k Inhabitants	Check the percentage that represents the value of the contract divided by 100k inhabitants
FQ16	Contract Value by Agency	Check the percentage that represents the value of the contract in relation to the agency's budget
FQ17	Inactive CNPJ	Check if the company registration number (CNPJ) is inactive.
FQ18	Tax Regime vs. Contract Value	Check if the value of the contacts falls within the tax regime described by the company
FQ19	Companies Donating to Political Campaigns	Check whether the company has donated any amount to political campaigns in recent years
FQ20	Partners Donating to Political Campaigns	Check whether any of the partners' members have donated any amount to political campaigns in recent years
FQ21	Members Participating in Political Parties	Check whether any of the partners are members of any political party
FQ22	Company that provided services to any electoral campaign	Check whether the company provided services to any political campaign
FQ23	Ineligible Company (CGU)	Check the company's suitability before the CGU
FQ24	Ineligible Company (TCU)	Check the company's suitability before the TCU
FQ25	Punished Company (CGU)	Check the company's punishment before the CGU
FQ26	CNAEs associated with the company	Check whether the CNAEs associated with the company match the sale reported in the contract

Table 6.3: Red Flags Questions

The results of the questionnaire applied to Brazilian auditors revealed a high level of agreement with the proposed red flags, consolidating the practical validity of these indicators in detecting fraud in PP. Most participants considered the red flags relevant and applicable, highlighting their usefulness in identifying patterns and behaviors associated with fraudulent practices. This convergence between the proposed indicators and the auditors' experience reinforces the methodological adequacy adopted in the study. It highlights the potential of red flags as practical tools for combating irregularities.

In addition, the auditors provided qualitative insights that complemented the quantitative responses, allowing for the refinement of the red flags and the identification of possible improvements. Specific comments pointed to the need for additional data cross-referencing in some cases, but without compromising the overall reliability of the indicators. This practical evaluation reinforces the relevance of the proposed red flags and demonstrates the importance of incorporating professional perspectives in creating more robust and contextualized fraud detection models.

6.2.1.1 Qualitative insights from auditors

All qualitative justifications provided by participants in the questionnaire are presented and analyzed in this subsection, organized according to the corresponding evaluation di-

mensions addressed in the instrument. This structure enables a systematic examination of auditors' comments, reflections, and suggestions, complementing the quantitative Likert-scale responses and providing contextual depth to the empirical findings. By incorporating these professional insights, the analysis moves beyond numerical aggregation and captures the institutional reasoning that underpins auditors' assessments, thereby reinforcing the practical relevance and interpretative richness of the study's results.

Datasets

• Q5: Bolsa Família - Payments

- It may be through cross-referencing of company owners who bid with the government to identify potential front-persons in shell companies to circumvent competition.
- Outdated data from 2021 becomes inefficient.
- Possible lack of definition of Bolsa Família recipients with service providers, suppliers of budgets for public administration, for example.
- Indication of front-persons.
- Important information.
- I do not work with the subject and therefore cannot answer.
- It is an important database to be compared with potential bidders and buyers in order to discover any inconsistencies. It can be used to provide several audit lines.
- A person who receives Bolsa Família would not be able to be a partner in bidding companies.
- Identify front-persons in shell companies.
- For fraud checking, the set is relevant. It is possible to perform an analysis, validating some points, such as the benefit amount, the NIS code with the CPF, etc. It is also possible to combine this database with others, for example, SISOB, to see if there are deceased individuals receiving the benefit or even with RAIS and CAGED to check if the person's income is compatible with the benefit they are listed to receive.
- Potential beneficiaries of the Program may appear as responsible parties of bidding companies.

- Cross-referencing data between Bolsa Família information and other databases (Caged, HR system of civil servants, data on deceased individuals, among others) leads to the identification of possible fraud in the information contained in Bolsa Família.
- The data set covers a universe that is not so specific to public procurement.
- A beneficiary of a social program contracting with the government is a strong indication of fraud.
- A lot of fraud.
- Possibility of cross-referencing data with other corporate systems of the Federal Government in order to cross-referencing data with the aim of identifying fraud in the acquisition of the citizen's right.
- It is possible to cross-reference CPFs that are receiving the benefit with data from the audit object.

- **Q6: TSE**

- For research on company owners, partners or related parties and their connections, especially as campaign donors
- Data from 2024.
- Relationships with political groups.
- Important information.
- I do not work on this topic and therefore cannot answer.
- Another important, reliable and public database to ratify data originally reported.
- They are mainly relevant if combined with other databases where they have a common field to cross-reference data on relevant risks of the process. Whatever it may be...
- Potential political agents and unelected candidates may appear as responsible for bidding companies.
- The indicated link refers to a set of 161 databases, also of a non-intrinsic nature, but additional to the topic.
- Beneficiary of social program donating to political or party campaigns and money laundering.

- Lots of fraud.
- This is data from the electoral court on electronic voting machine software and not on public purchases.
- With the data made available, I believe that the auditor is not able to point out fraud or possible fraud.

- **Q7: CATMAT/CATSER**

- Help with product standardization and comparison
- Comparative standards
- I don't know
- I don't work on the subject and therefore I don't know how to answer.
- These isolated databases don't seem to be relevant to fraud checking. If they are combined with other databases, yes.
- It provides precision in defining values for configuring overpricing and over-billing.
- It refers to an outdated database (2020).
- Objective description of the material by its technical specifications.
- Identifies the characteristic of the item that was purchased with the item delivered.
- This is a registration of materials and services for subsequent public purchase
- What really happens with CATMAT/CATSER codes is that there are a huge number of codes for the same material/service, which makes it very difficult to standardize materials and services. Another important factor is the "inattentive" way in which the public agent defines the code, which often comes with a very different description of the requested/desired material. Suggestion: Drastically reduce the number of codes.
- Allows you to assess the quality of the objects purchased and compare them with each other

- **Q8: Contracts (GOV BR Contracts)**

- Supports the identification of similar contracts and comparisons for analysis purposes

- Difficulty opening the file, too heavy or defective.
- Important information
- Confirms the existence of previous and/or current contracts signed by certain CNPJ and/or public entity
- Very likely
- Allows the evaluation of the operational capacity of companies, based on the existence of other contracts signed.
- Verifies the qualification to execute contracts and how long the contract has been performed.
- Reveals important data for the audit to check
- The system in question has a multitude of available data that are very useful to the Auditor, enabling the cross-referencing of data from public contracts.

- **Q9: Companies (CNPJ Registration)**

- Analysis in conjunction with other databases of partners or representatives.
- A lot of data still to be opened. I was unable to open the data. Some difficulty with the file, heavy.
- Important information.
- Important database for circulating information (registration) about a given company.
- Database of great importance for conducting trails. Identifying the registration status of companies, address, partners.
- Yes. Very important for combining with other databases.
- Allows for evaluating the operational capacity of companies (address, size), as well as the profile of those responsible.
- Partners and fronts versus social programs, etc.
- Various important information such as partners in common, etc.
- Facilitates consultation of data on companies and their respective owners.

- **Q10: Unreliable Companies**

- History of participating companies.

- Very good, easy to access. But the file is heavy to open.
- Important information.
- Consult companies that are prohibited from contracting with the Public Administration (federal, state, municipal or DF).
- Yes. Very important to combine with other databases.
- Allows you to identify the participation of penalized companies in bids from other subnational entities.
- Identify companies that are prohibited from contracting with the public administration.
- To check if the public administration is contracting with prohibited or unsuitable companies.
- There is already a legal provision for consulting the TCU's certificate of unsuitable bidders before contracting any company.

- **Q11: Unreliable and Suspended Companies**

- History of participating companies.
- Very good, easy to access. But the file is heavy to open.
- Important information.
- Consult companies that are prohibited from contracting with the Public Administration (federal, state, municipal or DF).
- Yes. Very important to combine with other databases.
- Allows you to identify the participation of penalized companies in bids from other subnational entities.
- Identify companies that are prohibited from contracting with the public administration.
- To check if the public administration is contracting with prohibited or unsuitable companies.
- There is already a legal provision for consulting the TCU's certificate of unsuitable bidders before contracting any company.

- **Q12: Punished Companies**

- History of participating companies.

- Very good, easy to access. But the file is heavy to open.
- Important information.
- Check whether the company has already received any punishment from the CGU, based on the LAC.
- Allows you to identify the participation of penalized companies in bids from other subnational entities.
- Identify and prevent companies from contracting with the public administration.
- Check possible restrictions on the future contractor.
- Makes it easier to check for unsuitable companies before hiring.

- **Q13: Suppliers**

- History of companies participating in various agencies for cross-analysis.
- Important information.
- Check whether the company has already signed a contract with the government - or participated in competitions.
- Allows for the evaluation of the operational capacity of companies (address, size).
- Qualification of suppliers, etc.
- List of suppliers of a specific material or service.
- I am unfamiliar with the system.

- **Q14: Invoices**

- Identify irregular pricing or supply after purchases.
- Easy access, but the file does not open, it seems heavy.
- Important information.
- Check if the company has already issued an invoice to the Public Administration, to then check if the invoice is valid.
- Allows you to evaluate the operational capacity of companies, their line of business, as well as the supply history and respective prices charged.
- Ability to supply goods and services, as well as identify fraud in invoices and is used for price research.

- Survey of prices charged to compile a market price spreadsheet or to check for unfeasibility.
- I am not familiar with the functionality, although I am familiar with the portal.

- **Q15: Safra Guarantee**

- For subsidiary analyses of participants or company owners.
- Easy access, but the file does not open, it seems heavy.
- I do not know it.
- I have not seen any use for it yet.
- I am not familiar with the functionality, although I am familiar with the portal.

Red Flags

- The ID card must be easily accessible, and the files must be easy to open.
- Atricon Transparency Radar.
- History of partners of companies contracted by the government, to check for possible concealment of a public agent or other type of agent who is prevented from providing goods or services to the public agency/entity.
- Database of fishermen's registration. Rais/Caged. CPF.
- Database of Deceased Persons. Very important in this type of process.
- National Public Procurement Portal.
- ITR, RAIS, CadUnico, e-Social, Purchasing Courts, other electronic purchasing sites existing in the public administration.
- No.

6.2.2 Case technical evaluation

This stage of the evaluation consisted of a structured technical assessment of anonymized public procurement cases that presented potential fraud indicators. Nine experienced auditors participated in this phase, examining six real cases that were previously anonymized to preserve confidentiality. For each case presented, participants were asked to provide

their professional judgment regarding the degree of suspicion, identify which red flags they considered relevant, and evaluate the adequacy of the automated classification produced by the referenced model. The objective was not to establish definitive fraud confirmation, but rather to compare professional judgment with model-generated signals and examine their alignment within a controlled analytical setting.

The evaluation instrument combined structured response items with open-ended fields, allowing auditors to justify their assessments and explain the reasoning underlying their decisions. Participants were encouraged to describe the technical criteria they applied, highlight contextual factors influencing their judgment, and comment on the pertinence of the red flags activated by the model. These qualitative justifications provide critical insight into how domain experts interpret risk signals and assess automated outputs, enabling a deeper understanding of convergences, divergences, and potential areas for refinement in the referenced model. Participation was voluntary, and all responses were collected anonymously to ensure confidentiality and encourage candid professional evaluation.

For each anonymized case presented, the evaluation instrument followed a structured sequence of questions designed to capture both quantitative judgments and qualitative reasoning. Auditors were first asked to indicate the degree of suspicion associated with the case using an ordinal scale ranging from “not suspicious” to “very suspicious,” including neutral and abstention options. Subsequently, they were invited to assess whether the case should be investigated further and, if so, at what priority level, thereby capturing the operational implications of their suspicion judgment. In addition, participants evaluated the relevance of each red flag activated in the case through a Likert-type matrix, indicating the perceived importance of each indicator in supporting suspicion. They were also asked to assess the adequacy of the automated classification provided by the referenced model (e.g., high risk), using a graded agreement scale. Finally, an open-ended comment field was provided for each case, allowing auditors to justify their decisions, elaborate on contextual considerations, and offer technical observations. This structured design enabled the collection of multidimensional assessments that combine suspicion grading, prioritization logic, indicator relevance, model agreement, and qualitative reasoning.

6.2.2.1 Case 1

Case 1 refers to the contracting, without bidding, of document management services by the Ministry of Labor and Social Security (General Coordination of Logistics Resources –

CGRL), in the amount of R\$ 3,728,516.00, carried out on January 4, 2024. The automated analysis identified a set of red flags with strong institutional sensitivity, including the existence of a prior contractual link with a political party, the status of a partner who donated to an electoral campaign, the presence of a partner holding an active public office, and the temporal proximity between the company’s incorporation and the signing of the contract. The combination of these elements suggests a potential risk of conflict of interest, undue favoritism, or political instrumentalization of public procurement. Given the convergence of these indicators, the system classified the case as high risk, with a high level of confidence (98%), signaling priority for evaluation by control bodies.

Figure 6.4 presents the perceived degree of suspicion attributed to the case. The results indicate a strong convergence toward high suspicion, with 88.9% of auditors classifying the case as *very suspicious* and 11.1% as *suspicious*. No respondent considered the case neutral or non-suspicious. This near-unanimous assessment suggests a high level of institutional concern, aligning with the activation of multiple politically and institutionally sensitive red flags.

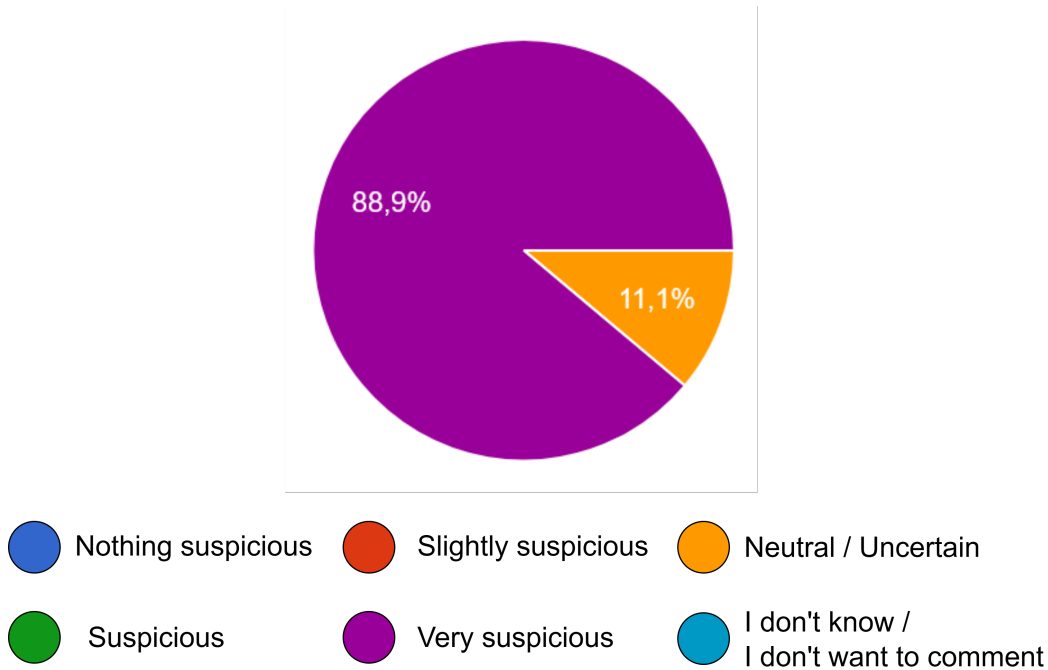


Figure 6.4: Auditor Perceived Degree of Suspicion (Case 1)

Figure 6.5 illustrates the priority assigned for further investigation. A majority of auditors (66.7%) indicated that the case should be investigated with high priority, while 22.2% recommended maximum priority and 11.1% indicated medium priority. None of the respondents suggested low priority or refraining from investigation. These findings demonstrate that suspicion judgments translated into concrete operational implications,

reinforcing the perceived relevance of the case within oversight routines.

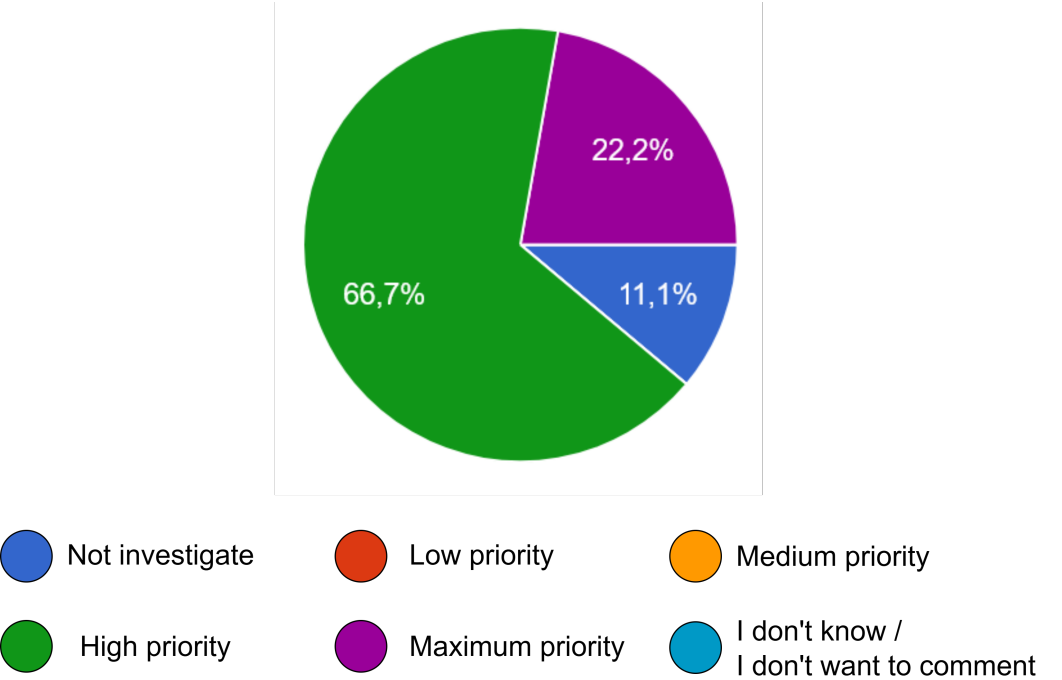


Figure 6.5: Investigation Priority Assessment by Auditors (Case 1)

Figure 6.6 presents the perceived relevance of each activated red flag. Political linkage indicators, particularly the company’s association with a political party and campaign donation records, received predominantly high or extreme relevance ratings. The presence of a partner serving as an active public official was also evaluated as highly relevant by most respondents. The temporal proximity between company creation and contract award showed slightly more dispersion, though it was still largely considered of high or extreme importance. This distribution indicates that auditors interpret the combination of political exposure and institutional conflict indicators as particularly salient risk signals.

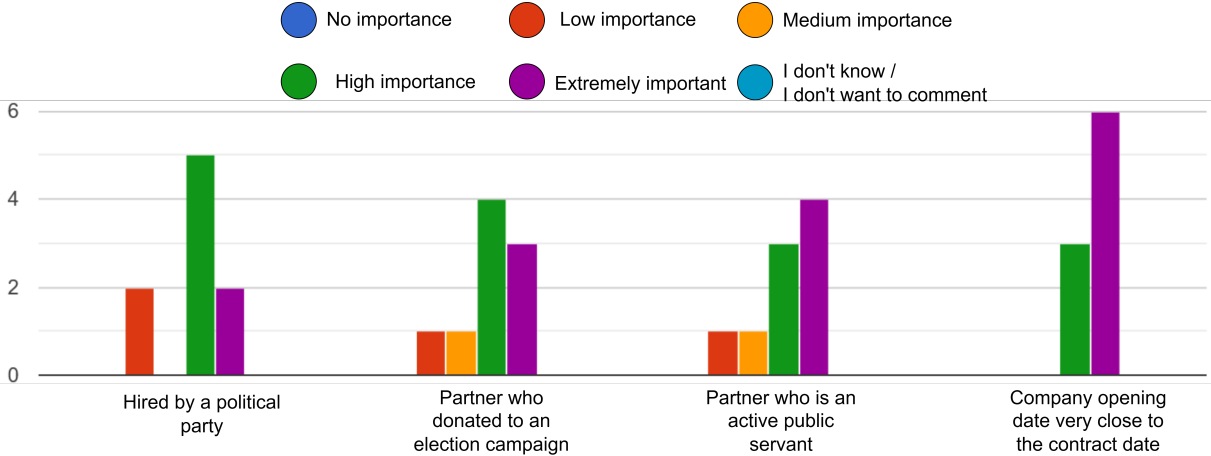


Figure 6.6: Perceived Relevance of Activated Red Flags (Case 1)

Finally, Figure 6.7 reports auditor agreement with the automated classification of the case as high risk. A substantial majority (88.9%) expressed total agreement with the system's classification, while 11.1% indicated partial disagreement. No neutral or strong disagreement responses were recorded. This result reveals a high degree of alignment between professional judgment and the referenced model's output, suggesting that, for this case, the automated risk assessment reflects institutional reasoning patterns commonly applied in practice.

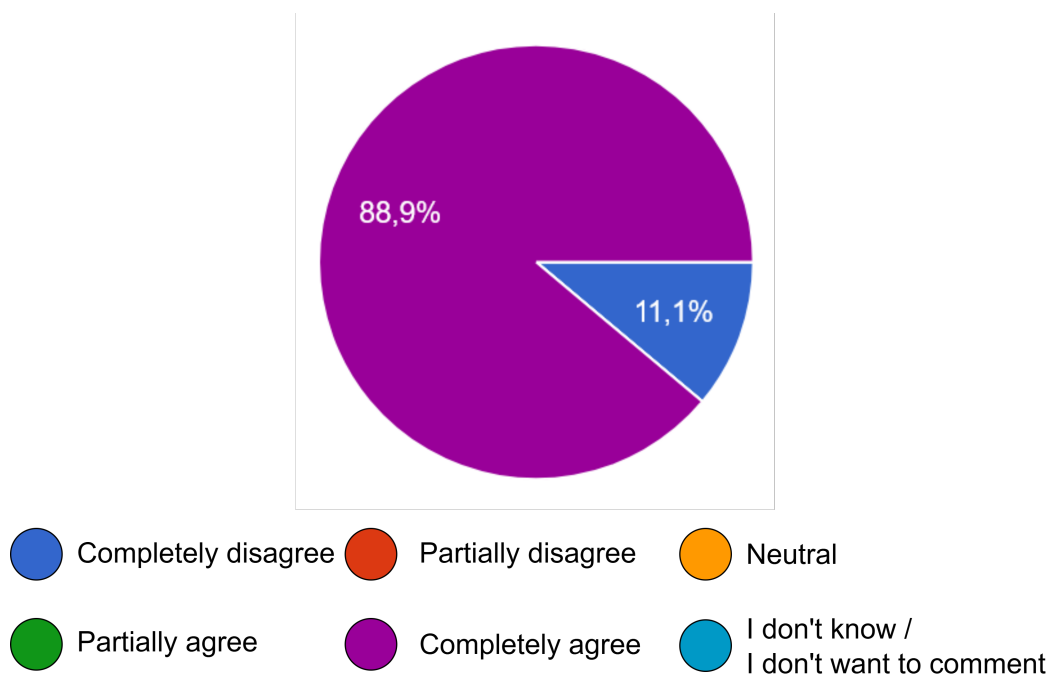


Figure 6.7: Auditor Agreement with Model Classification (Case 1)

The qualitative comments provided by auditors, presented in bullet format below, emphasize that the identified red flags should be interpreted as indicative signals rather than definitive evidence of fraud. Respondents highlighted the importance of analyzing these indications in conjunction with additional contextual elements before motivating formal control actions. Some auditors stressed that the concurrence of multiple relevant indicators elevates the perceived risk, while others raised practical considerations regarding data sourcing and proportionality of contract value within the institutional context. Overall, the comments reinforce the interpretative and contextual nature of professional judgment in fraud risk assessment.

- These are only indications. They must be analyzed in conjunction with other elements. These indications alone do not motivate any control action.

- There is a concurrence of relevant indications, not just one. Therefore, the case has a risk classification above average.
- The red flag about being contracted by a Political Party is interesting. My question is how to obtain this information.
- The fact that it is a newly opened company, with little service history, and was contracted through a waiver points to possible undue influence by a partner who is a public servant. I wouldn't give it maximum priority because the value, considering it's a central agency's logistics sector, appears to be proportionally low – but I could only make such an assessment with knowledge of the scale of values executed by the agency.

6.2.2.2 Case 2

Case 2 involves a contract awarded without bidding by the Regional Electoral Court of Pará (TRE/PA), for R\$ 16,260.00, for the execution of classes and workshops linked to the "Political Training School" project, with the commitment registered on February 14, 2025. The analysis identified as red flags the fact that one of the partners of the contracted company is a beneficiary of a social program and affiliated with a political party. Although the contracted value is relatively low, the political ties associated with the object—directly related to political training—may raise questions regarding impartiality, the potential overlap between partisan and institutional interests, and the suitability of the supplier's selection. Considering the combination of these elements, the system classified the case as high risk, with 97% confidence, indicating the need for contextualized evaluation by the control bodies.

Figure 6.8 presents the perceived degree of suspicion attributed to Case 2. In contrast to Case 1, the distribution of responses reveals greater dispersion in auditors' judgments. Specifically, 33.3% classified the case as *not suspicious*, 33.3% as *slightly suspicious*, 22.2% as *suspicious*, and 11.1% as *very suspicious*. No respondent selected the extreme "extremely suspicious" category. This distribution indicates the absence of strong consensus and suggests that, despite the activation of political linkage red flags, auditors interpreted the contextual elements—particularly the low contract value and the nature of the object—as mitigating factors in their suspicion assessment.

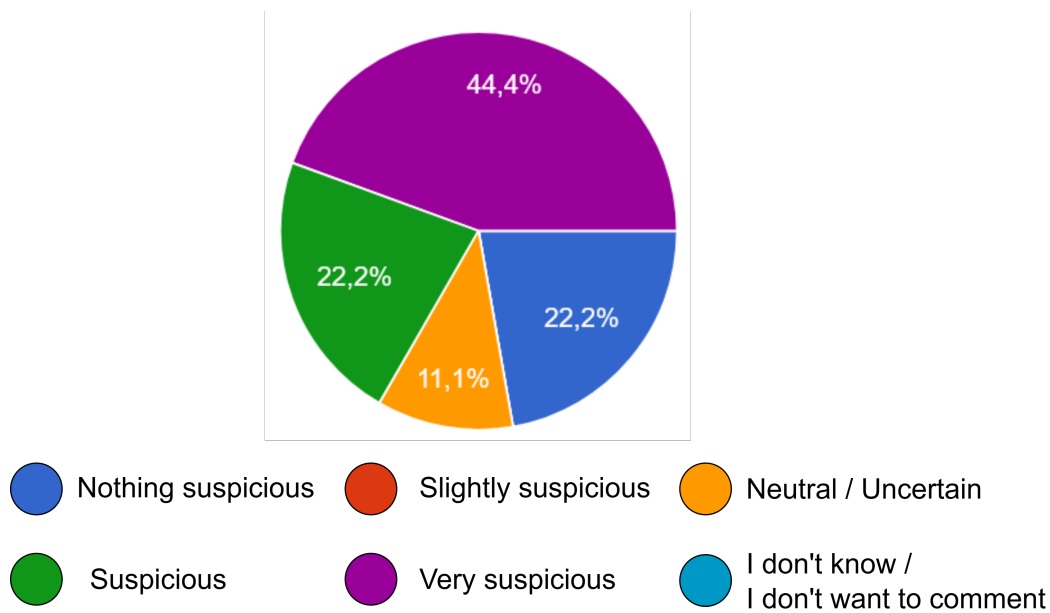


Figure 6.8: Auditor Perceived Degree of Suspicion (Case 2)

Figure 6.9 illustrates the priority assigned for further investigation. The results demonstrate a predominance of low operational urgency: 44.4% of auditors indicated that they would not investigate the case, 22.2% suggested low priority, 22.2% moderate priority, and only 11.1% high priority. No respondent recommended maximum priority. This outcome reinforces the notion that suspicion perception does not automatically translate into investigative escalation, especially when materiality thresholds are considered low. The case illustrates how professional judgment incorporates proportionality principles within oversight routines.

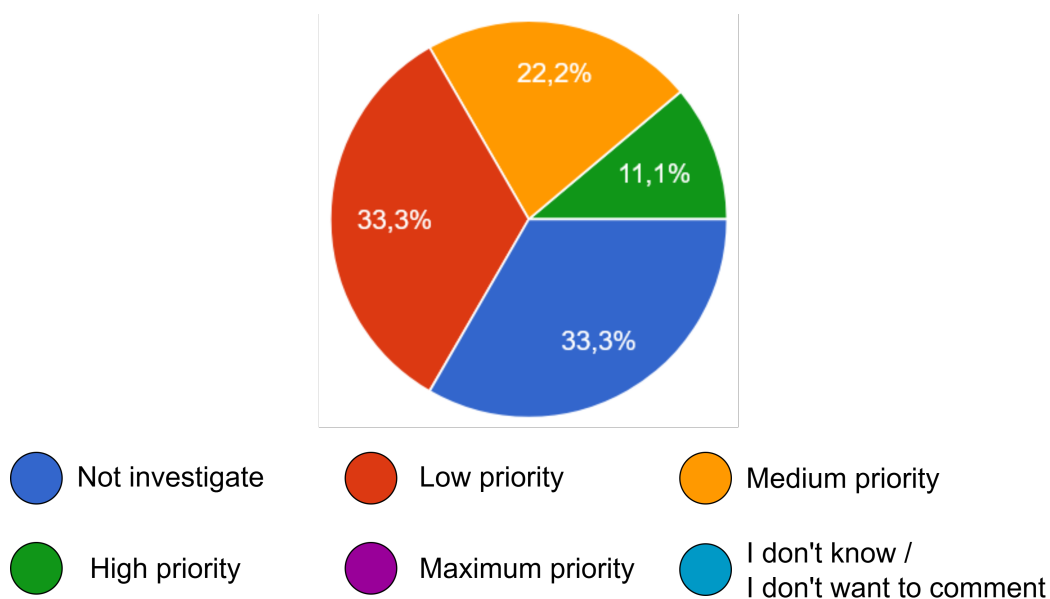


Figure 6.9: Investigation Priority Assessment by Auditors (Case 2)

Figure 6.10 presents the perceived relevance of each activated red flag. The political affiliation of the partner received more polarized evaluations, with responses distributed across low, medium, and high relevance categories. The indicator concerning the partner being a beneficiary of a social program was largely considered of low or medium importance. Overall, neither red flag achieved dominant “high” or “extreme” relevance ratings. This distribution suggests that auditors interpreted these signals as context-dependent and insufficient, in isolation, to justify a strong risk classification.

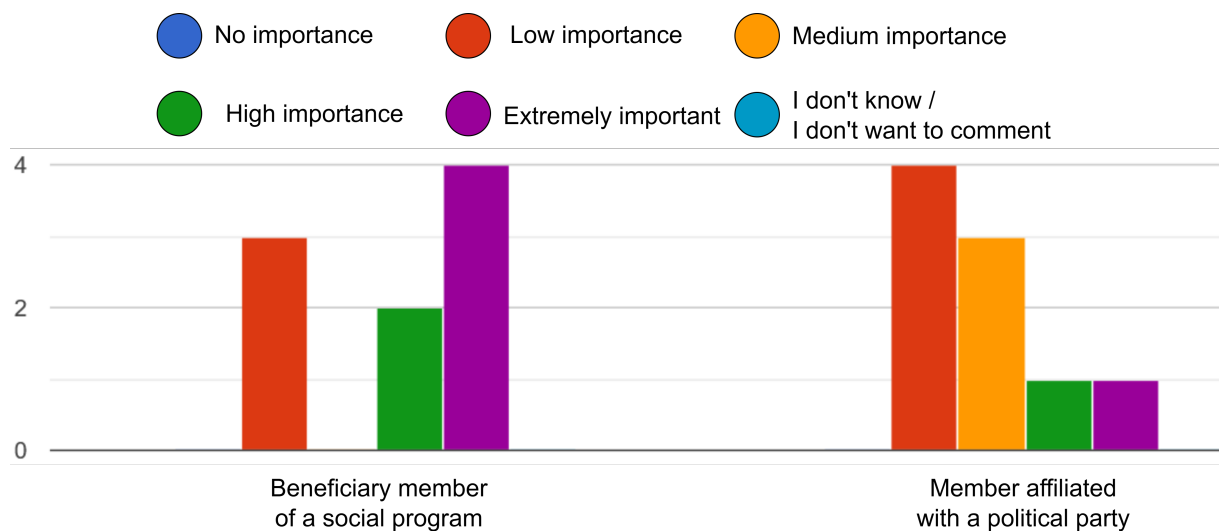


Figure 6.10: Perceived Relevance of Activated Red Flags (Case 2)

Finally, Figure 6.11 reports auditor agreement with the automated classification of the case as high risk. Agreement levels were moderate and heterogeneous: 33.3% totally agreed with the system’s classification, while 22.2% partially agreed, 22.2% partially disagreed, and 22.2% totally disagreed. This balanced dispersion contrasts sharply with Case 1 and indicates limited alignment between the model’s output and institutional reasoning in contexts of low materiality and ambiguous red flag interpretation. The findings highlight a boundary condition of the reference model: when risk signals lack material weight or contextual reinforcement, automated high-risk classifications may be perceived as disproportionate.

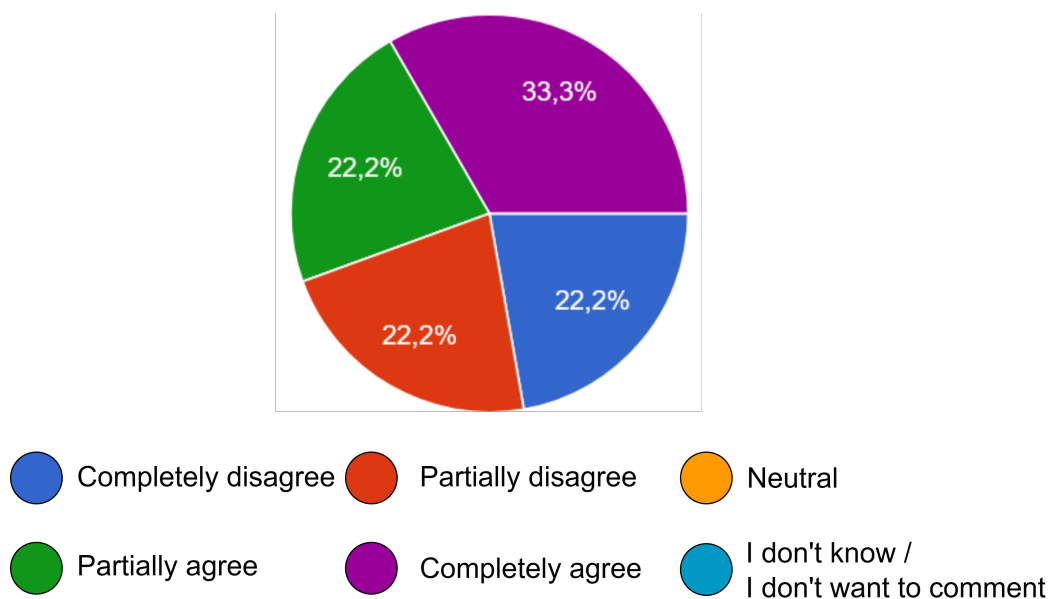


Figure 6.11: Auditor Agreement with Model Classification (Case 2)

The qualitative comments provided by auditors, presented below in bullet format, reinforce this interpretative nuance. Respondents emphasized that the identified indicators do not automatically justify high-risk classification and must be contextualized within materiality, sector characteristics, and additional evidentiary elements. Several auditors noted that political affiliation may be compatible with the nature of the contracted service (a political training initiative), and that being a beneficiary of social programs does not, in isolation, constitute a meaningful fraud indicator. Materiality was repeatedly cited as a decisive factor, with auditors indicating that the relatively low contract value would limit investigative priority even if stronger red flags were present. Overall, the comments highlight proportionality, contextual reasoning, and evidentiary sufficiency as central elements of professional judgment in this case.

- Similar to the previous answer.
- Here it is verified that there is a high probability that the partner is a front man, however, other elements would be needed for the risk to be high, such as an excessive number of CNAEs (National Classification of Economic Activities), registrations in CNEP (National Registry of Economic and Social Security Numbers) or CEIS (Cadastro Nacional de Empresas Social - National Registry of Business Entities).
- The low priority in the investigation stems from the low materiality.
- The political ties of the partner of the supplier company may be related to the nature of the services provided (political training school). The fact that the partner

is a beneficiary of social programs in isolation says nothing, as the company may have low revenue and/or low share capital. The low materiality of the value would prevent me from taking any investigative action, even if there were more compelling red flags.

6.2.2.3 Case 3

Case 3 refers to an electronic auction held by the Army Command – Administrative Base of the Special Operations Command, valued at R\$ 100,000.00, for the contracting of neuropsychological assessment and applied behavior analysis (ABA) services, formalized on December 27, 2024. Despite being a competitive modality, the analysis identified relevant red flags: the company has a high frequency of previous contracts awarded without bidding, is listed in the National Registry of Punished Companies (CNEP), and has a CNAE (National Classification of Economic Activities) code incompatible with the service provided. The combination of these factors suggests potential registration inconsistencies and risks related to the supplier's integrity and technical capacity. Given this set of indications, the system classified the case as high risk, with 96% confidence, indicating the need for in-depth verification regarding the company's qualifications, contractual history, and regularity.

Figure 6.12 presents the perceived degree of suspicion attributed to Case 3. The responses reveal a predominantly high level of concern: 66.7% of auditors classified the case as *very suspicious*, while 33.3% considered it *suspicious*. No respondent evaluated the case as neutral or non-suspicious. This distribution indicates strong convergence toward elevated suspicion, suggesting that the combination of compliance-related red flags—particularly the company's presence in the CNEP and inconsistencies in CNAE—triggered robust institutional alertness.

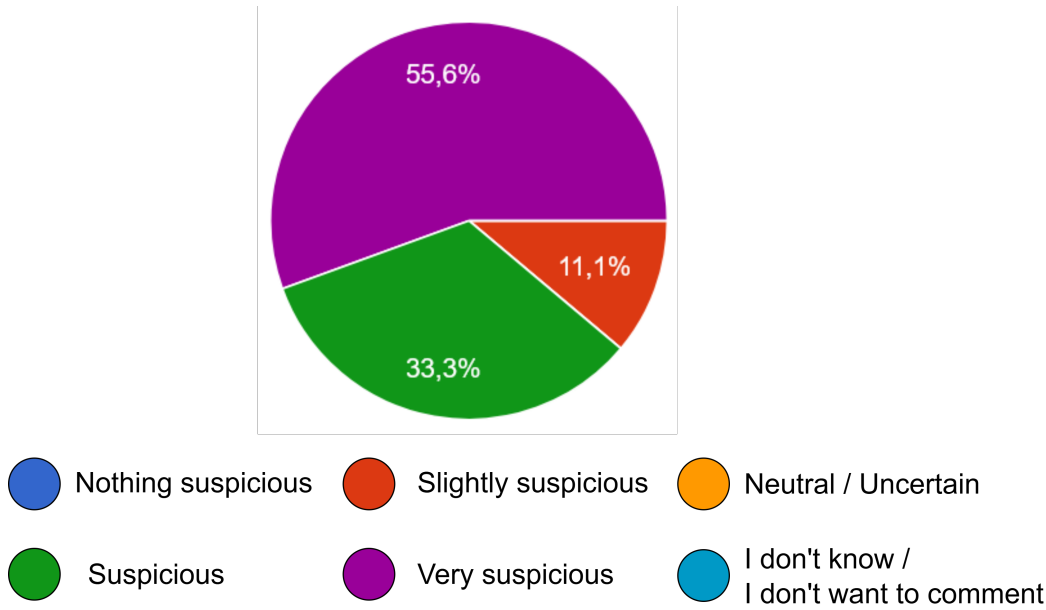


Figure 6.12: Auditor Perceived Degree of Suspicion (Case 3)

Figure 6.13 illustrates the priority assigned for further investigation. A majority of auditors (55.6%) recommended maximum priority, while 33.3% indicated high priority and 11.1% suggested medium priority. No responses indicated low priority or dismissal of investigation. Compared to previous cases, this distribution reflects an even stronger operational inclination toward immediate scrutiny, reinforcing that sanction-related indicators (e.g., CNEP listing) are interpreted as particularly severe within oversight practice.

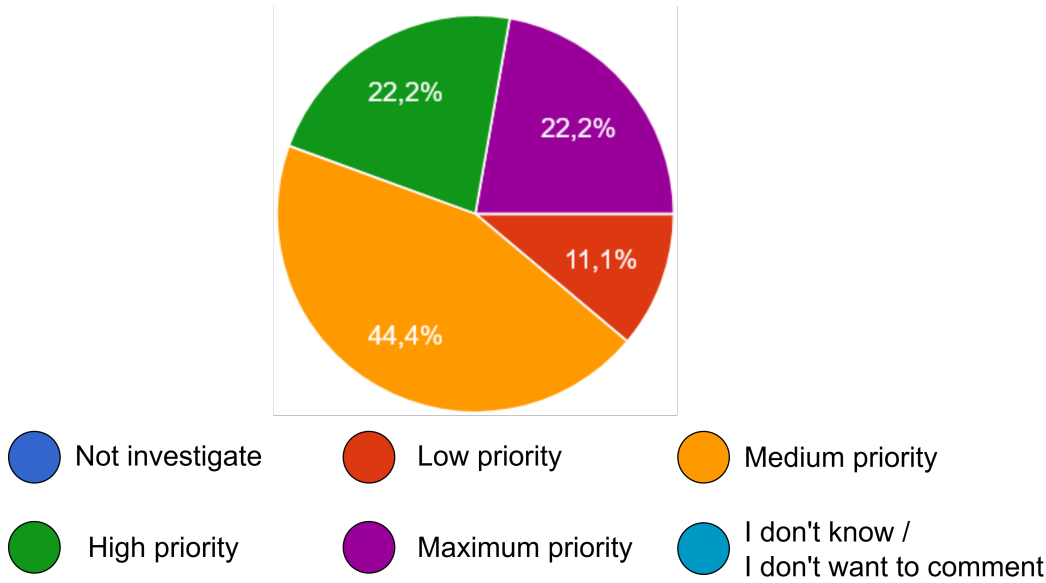


Figure 6.13: Investigation Priority Assessment by Auditors (Case 3)

Figure 6.14 presents the perceived relevance of each activated red flag. The company’s

presence in the Cadastro Nacional das Empresas Punidas (CNEP) received predominantly extreme relevance ratings, standing out as the most critical indicator. The mismatch between the company’s CNAE and the contracted service was also evaluated as highly relevant, while the high frequency of victories by waiver showed slightly more dispersion but remained largely rated as high or extreme importance. Overall, the distribution demonstrates that auditors assign greater weight to formal sanction records and structural inconsistencies than to behavioral procurement patterns alone.

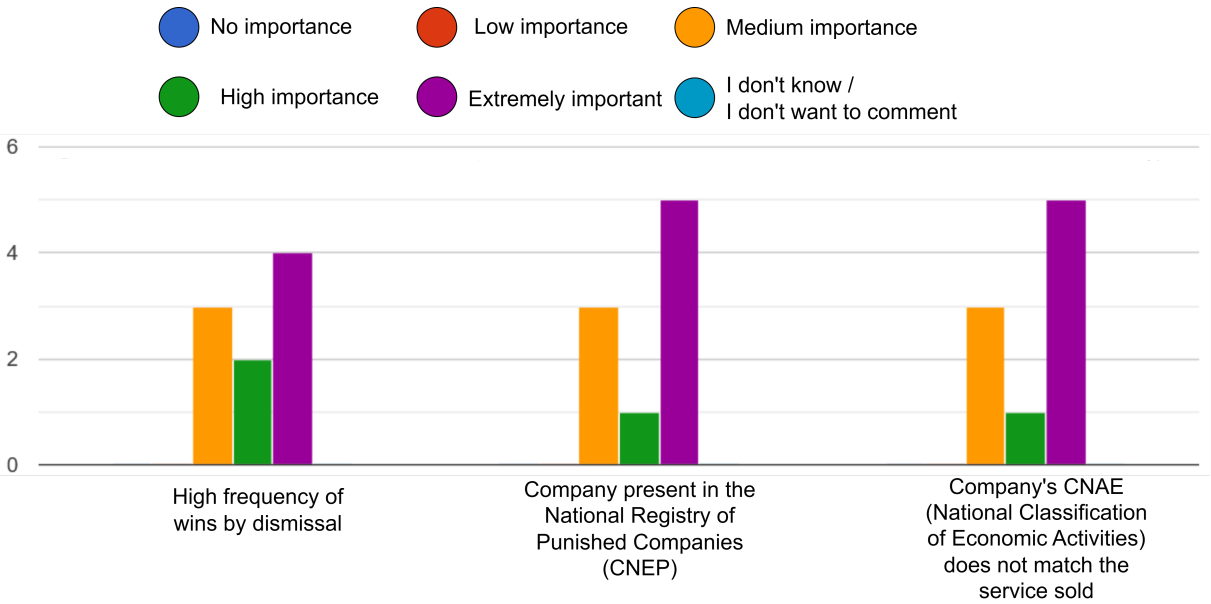


Figure 6.14: Perceived Relevance of Activated Red Flags (Case 3)

Finally, Figure 6.15 reports auditor agreement with the automated classification of the case as high risk. A substantial majority (66.7%) expressed total agreement with the system’s classification, while 33.3% indicated partial agreement. No disagreement responses were recorded. This pattern suggests a strong alignment between professional judgment and the referenced model’s output, particularly when the activated red flags involve objective compliance violations rather than interpretative political or socioeconomic indicators.

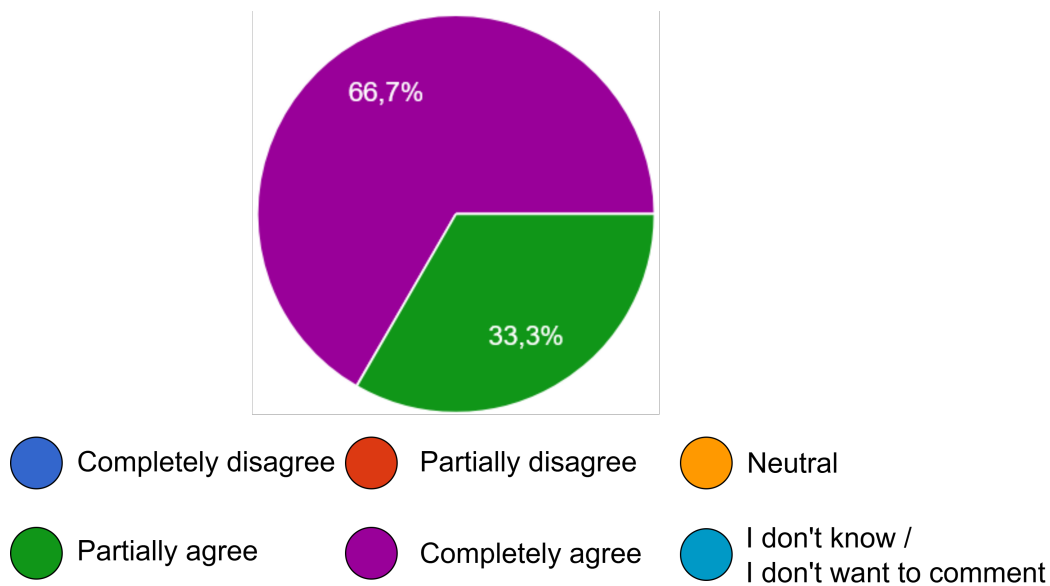


Figure 6.15: Auditor Agreement with Model Classification (Case 3)

The qualitative comments reinforce this interpretation. Auditors emphasized that the identified red flags are substantively aligned with high-priority investigation criteria, especially the CNEP listing, which in principle could constitute an impediment to contracting. At the same time, respondents highlighted the need to contextualize materiality and broader contractual history, stressing that proportionality and cumulative exposure remain relevant factors in deciding investigative allocation. Overall, Case 3 reveals a scenario in which sanction-based and structural inconsistencies generate strong institutional convergence and high alignment with the system's risk classification.

- Better evidence. They signal possible irregularities.
- Here the red flags are very well aligned for high prioritization.
- The fact that it is in the CNEP should be an impediment to the contracting, therefore, the company is being unduly benefited by the public contracting. However, depending on the context of the investigation team, the value of the contract is not materially relevant, in a first analysis. For a more assertive decision, it would be necessary to understand if the bodies that contract through exemption have any relation with the contracting portrayed in the hypothesis; as well as the total supply values of the company (considering the exemptions + the auction in question).

6.2.2.4 Case 4

Case 4 refers to a contract awarded without bidding by the Ministry of Economy – Directorate of Administration and Logistics, for R\$ 386,276.22, for the purchase of automotive fuel to supply official CNPq vehicles, formalized on August 7, 2023. Although the contractual object is recurrent in public administration, two relevant red flags were identified: the existence of a company partner with political involvement and share capital lower than the contracted value. These elements may indicate potential risks related to conflicts of interest and the supplier's economic and financial capacity. The combination of these factors led the system to classify the case as high risk, with 95% confidence, signaling the need for a more in-depth analysis regarding the company's corporate structure and financial compatibility with the size of the contract.

Figure 6.16 presents the perceived degree of suspicion attributed to Case 4. The responses indicate a heterogeneous distribution of perceptions. A plurality of auditors (44.4%) classified the case as *suspicious*, while 22.2% considered it *very suspicious*. At the same time, 22.2% evaluated the case as *little suspicious*, and 11.1% indicated a neutral position. No respondent classified the case as non-suspicious. This dispersion suggests that, although relevant red flags were identified, auditors weighted contextual elements—such as materiality and procurement modality—differently when forming their suspicion judgments.

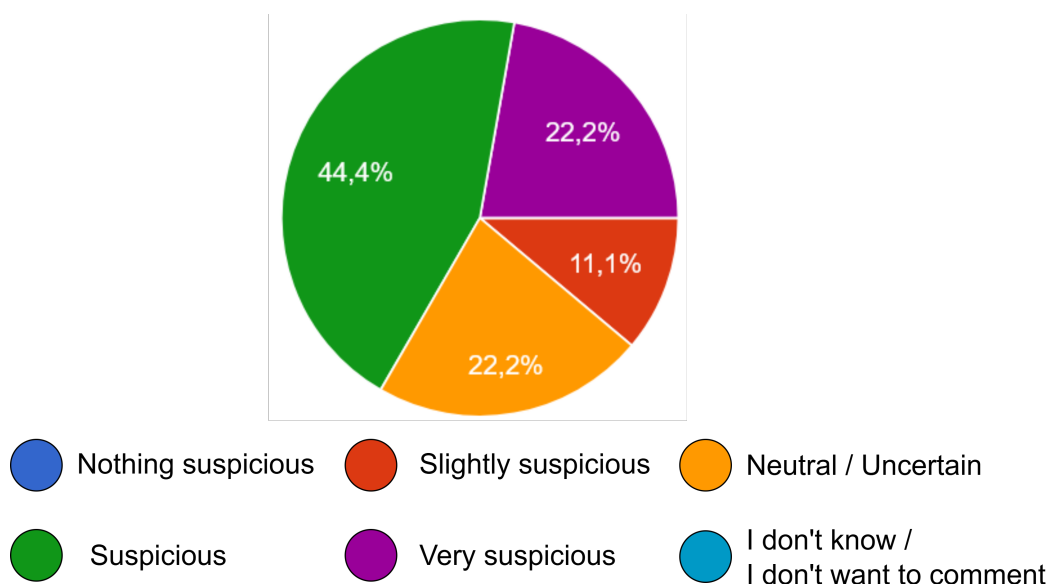


Figure 6.16: Auditor Perceived Degree of Suspicion (Case 4)

Figure 6.17 illustrates the priority assigned for further investigation. The results reveal a moderate inclination toward investigation, with 44.4% recommending high priority,

22.2% indicating medium priority, and 22.2% suggesting low priority. Additionally, 11.1% recommended maximum priority. No auditor opted to refrain from investigation entirely. These findings indicate that, while suspicion was not unanimous at the highest level, most auditors still considered the case worthy of oversight attention, particularly due to the political exposure indicator and the procurement modality adopted.

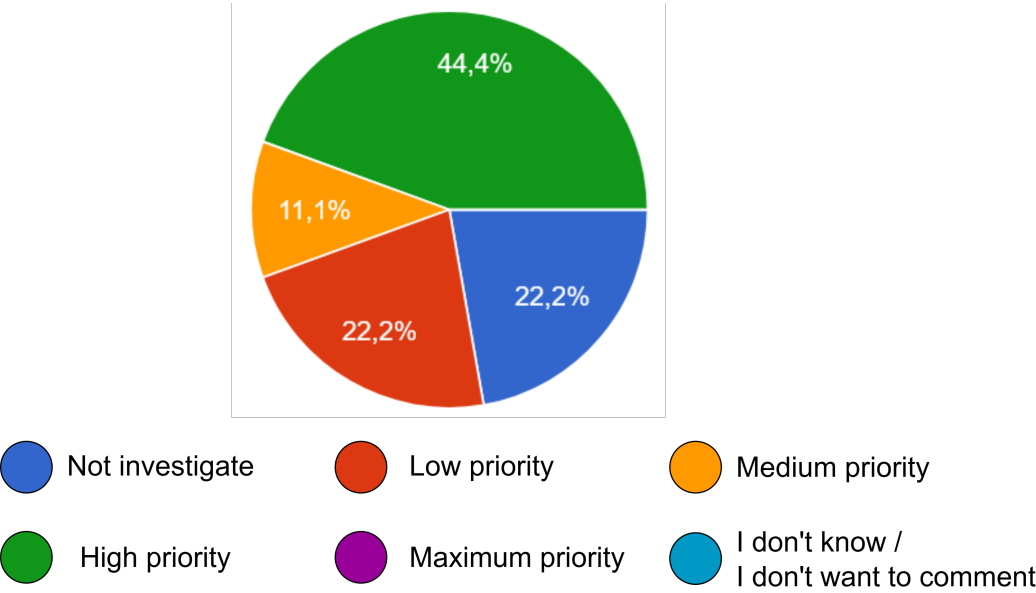


Figure 6.17: Investigation Priority Assessment by Auditors (Case 4)

Figure 6.18 presents the perceived relevance of the activated red flags. The indicator related to the company partner being an active politician received predominantly high or extreme relevance ratings, demonstrating strong institutional sensitivity to potential conflicts between political activity and public contracting. In contrast, the red flag concerning the company’s social capital being lower than the contract value exhibited slightly greater dispersion, with some auditors classifying it as moderately relevant. This pattern reflects the understanding that, while capital proportionality may signal risk, it often requires complementary evidence to substantiate a more severe assessment.

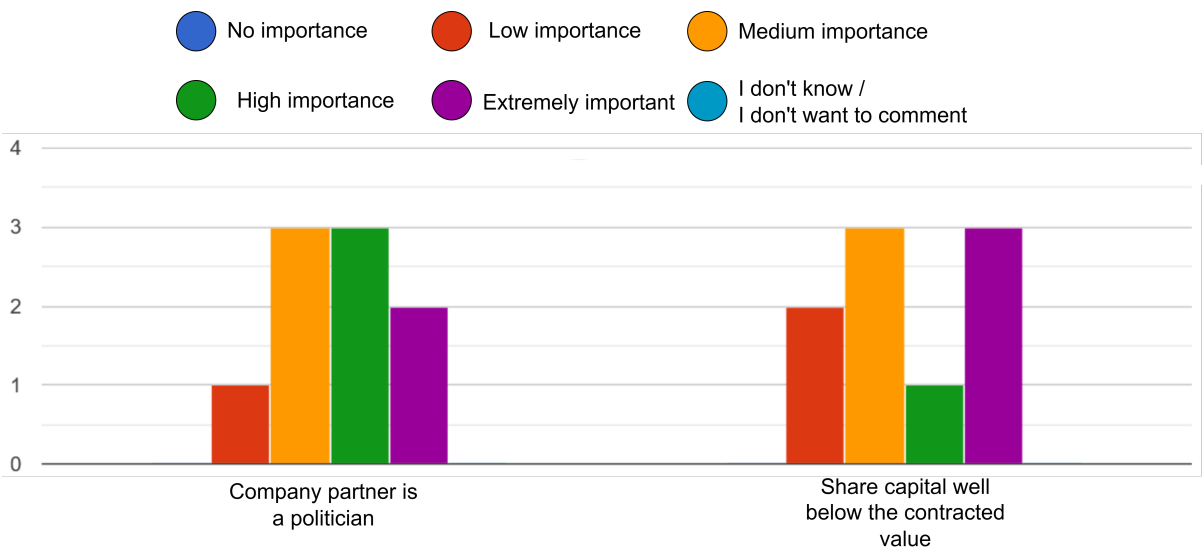


Figure 6.18: Perceived Relevance of Activated Red Flags (Case 4)

Finally, Figure 6.19 reports auditor agreement with the automated classification of the case as high risk. A majority (44.4%) expressed total agreement with the system's output, while 22.2% indicated partial agreement and 22.2% partial disagreement. A smaller portion (11.1%) expressed total disagreement. This distribution reveals a more divided alignment between professional judgment and the referenced model compared to cases with stronger convergence. The divergence appears to stem primarily from contextual considerations regarding materiality and the adequacy of the inexigibility modality, rather than from disagreement with the underlying red flags themselves.

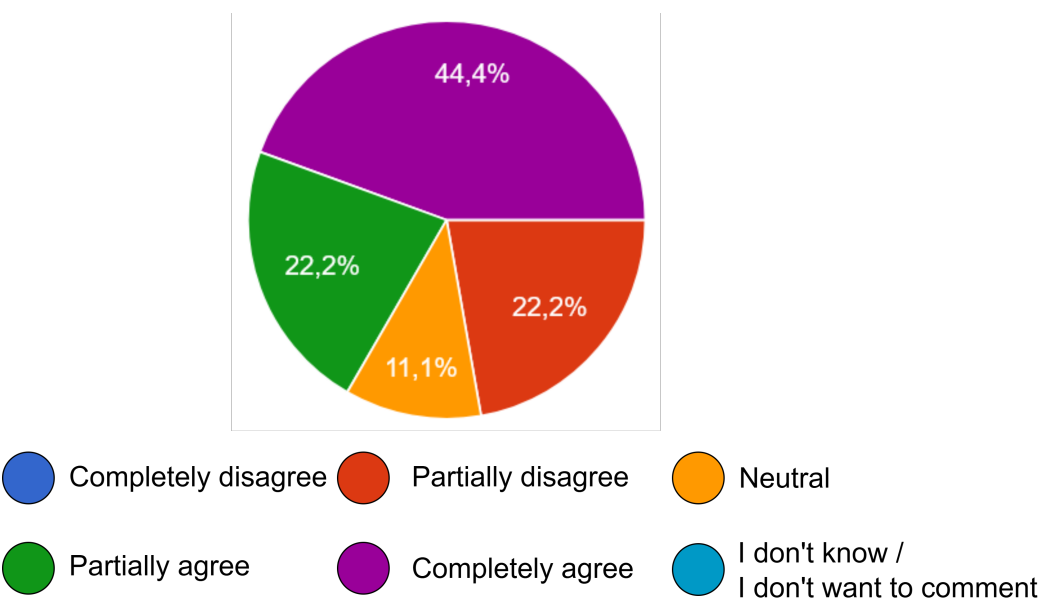


Figure 6.19: Auditor Agreement with Model Classification (Case 4)

The qualitative comments provided by auditors, presented in bullet format below, reinforce that the political exposure of a company partner is perceived as a strong institutional irregularity indicator, while low social capital is considered a complementary, but not decisive, signal. Respondents emphasized the need for convergent and concordant evidence to characterize irregularity, consistent with jurisprudential standards adopted by higher courts and courts of accounts. Additionally, some auditors questioned the appropriateness of the procurement modality (*inexigibility*) for the contractual object and highlighted that materiality plays a central role in determining investigative priority. Overall, the comments illustrate how legal interpretation, proportionality, and contextual financial relevance mediate the translation of red flags into control action.

- The fact that the partner is a politician indicates an irregularity, contradicting the federal constitution itself. The low share capital is indicative, but not fraud. In general, up to 10% of the estimated contract value can be required as share capital. This would only be an indication. To characterize irregularity, there would have to be a robust set of indications. Several, convergent and concordant. Higher courts and audit courts follow this line of reasoning.
- The object of the bidding process does not seem to qualify as a case of ineligibility.
- Here the red flags are strong, mainly because the partner has political activity.
- The priority is linked to materiality, but I would consider deepening the investigation.
- What would make me investigate would be the fact that the contract resulted from ineligibility. The effective action on the contract would depend on the context of the materiality of the expense. Apparently, for a central body, this value seems very low.

6.2.2.5 Case 5

Case 5 refers to an electronic auction conducted by the Ministry of Economy – Directorate of Administration and Logistics, valued at R\$ 19,648,000.00, for the contracting of continuous operational support services, including security, cleaning, maintenance, and gardening, formalized on November 1, 2025. This is a contract of high financial value and operational impact, intended for the maintenance of the administrative activities of the units served. The analysis identified as red flags the high frequency of previous wins

through exemption from bidding and the coincidence of registration data with two other companies in the same sector that also hold contracts with the government, which may suggest a possible corporate interrelation or coordinated action in the public market. Considering the combination of high contract value and potential indications of an atypical corporate structure, the system classified the case as high risk, with 94% confidence, recommending detailed verification regarding the corporate independence and the regularity of the company's participation in the bidding process.

Figure 6.20 presents the perceived degree of suspicion attributed to the case. The responses reveal a strong tendency toward high suspicion, with 66.7% of auditors classifying the case as *very suspicious*, 22.2% as *suspicious*, and 11.1% as *moderately suspicious*. No respondent considered the case neutral or non-suspicious. This distribution indicates a clear perception of elevated risk, likely influenced by the high contract value combined with structural red flags related to procurement patterns and corporate linkage indicators.

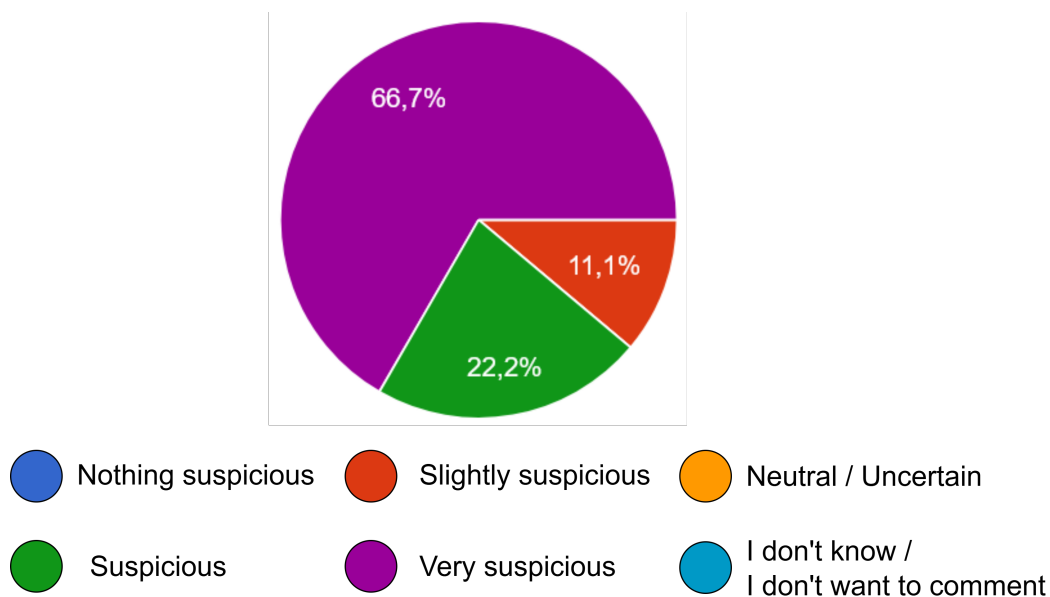


Figure 6.20: Auditor Perceived Degree of Suspicion (Case 5)

Figure 6.21 illustrates the priority assigned for further investigation. A majority of auditors (55.6%) recommended maximum priority, while 44.4% indicated high priority. No responses suggested medium or low priority. This near-consensus demonstrates that the combination of materiality (R\$ 19.6 million) and the concurrence of red flags translated directly into a strong operational recommendation for immediate investigative attention.

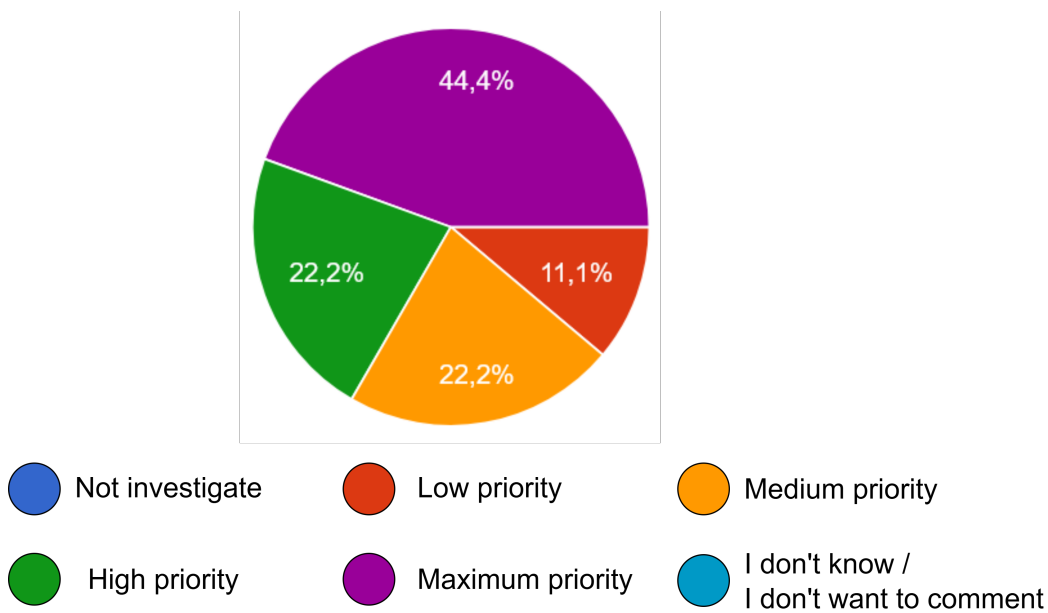


Figure 6.21: Investigation Priority Assessment by Auditors (Case 5)

Figure 6.22 presents the perceived relevance of each activated red flag. The indicator related to coincident corporate registration data with other companies operating in the same sector received predominantly high or extreme relevance ratings. Similarly, the high frequency of victories through waiver mechanisms was largely assessed as highly relevant. The distribution suggests that auditors interpret structural and relational inconsistencies—particularly those suggestive of coordinated corporate behavior or possible “shell company” configurations—as strong institutional risk signals.

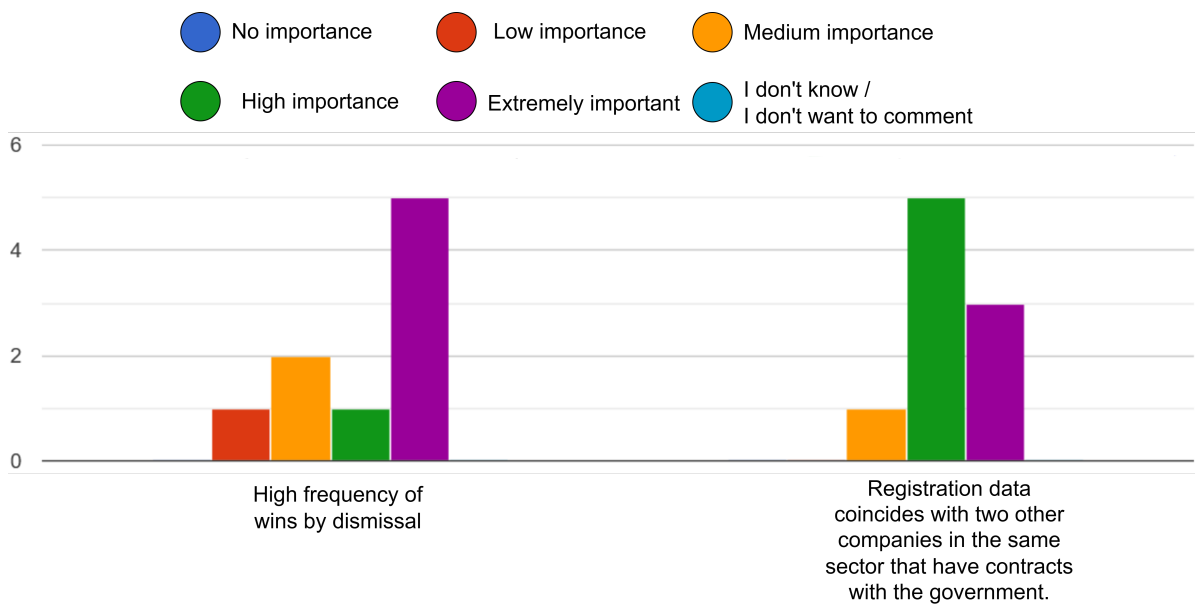


Figure 6.22: Perceived Relevance of Activated Red Flags (Case 5)

Finally, Figure 6.23 reports auditor agreement with the automated classification of the case as high risk. A majority (55.6%) expressed total agreement, while 44.4% indicated partial agreement. No neutral or disagreement responses were recorded. This result indicates strong alignment between the model's classification and professional judgment, although the presence of partial agreement responses suggests that auditors may still consider contextual elements—such as contractual execution details or historical performance—before fully endorsing the automated assessment.

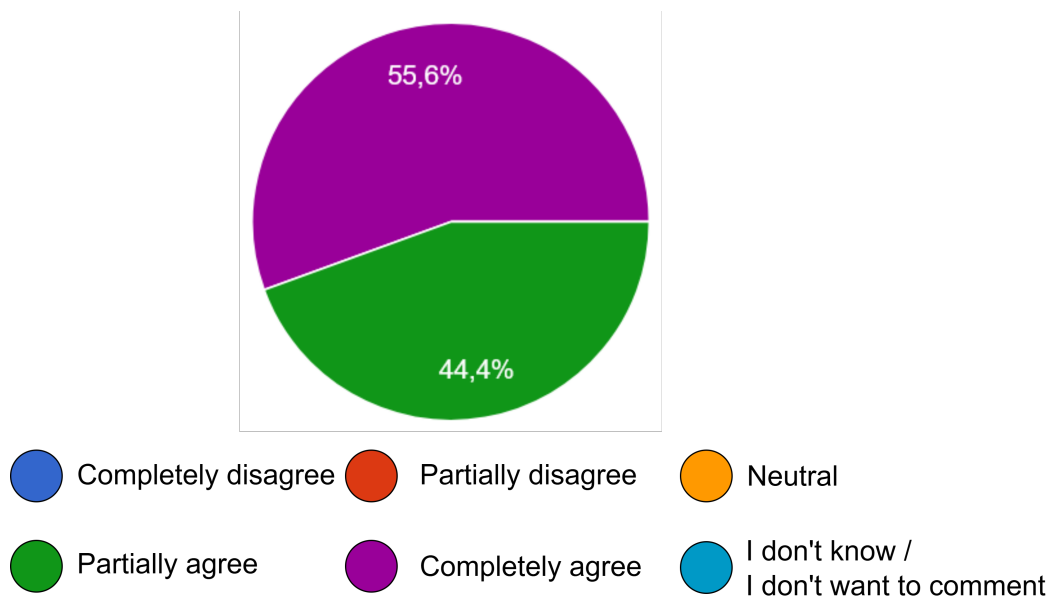


Figure 6.23: Auditor Agreement with Model Classification (Case 5)

The qualitative comment reinforces this interpretation. Auditors emphasized that the combination of high materiality, repeated waivers, and coincident corporate data constitutes a strong indication of potential shell-company arrangements requiring further investigation. The remarks highlight that structural convergence of red flags—particularly when associated with significant contract values—substantially increases institutional concern and justifies prioritization within oversight routines.

- In addition to the significant amount involved, the high number of exemptions and matching registration data are indications of a shell company that require investigation.

6.2.2.6 Case 6

Case 6 refers to a contract awarded through a waiver of bidding by VALEC – Engenharia, Construções e Ferrovias S/A, valued at R\$ 5,500,000.00, for consulting services to prepare

a proposal for corporate restructuring and reorganization, formalized on October 14, 2024. The strategic nature of the contract, coupled with its significant value and the use of the waiver modality, already constitutes a sensitive context from a governance perspective. The analysis identified as red flags the existence of a partner who is a donor to a political party and an electoral candidate, a high level of company participation in government contracts, and share capital lower than the contracted value. The combination of these elements may indicate risks related to potential political influence, significant dependence on public revenue, and economic and financial fragility relative to the size of the contract. Given this set of indicators, the system classified the case as high risk, with 93% confidence, signaling the need for in-depth examination of the regularity, technical capacity, and independence of the contracted company.

Figure 6.24 presents the perceived degree of suspicion attributed to the case. The majority of auditors (66.7%) classified the case as *very suspicious*, while 22.2% considered it *suspicious* and 11.1% rated it as *neutral*. No respondent classified the case as non-suspicious. Although there is slight dispersion when compared to cases with near-unanimous convergence, the results still indicate a strong perception of elevated fraud risk, particularly in light of the combination of political donations, high government contract participation, and disproportionate capital structure.

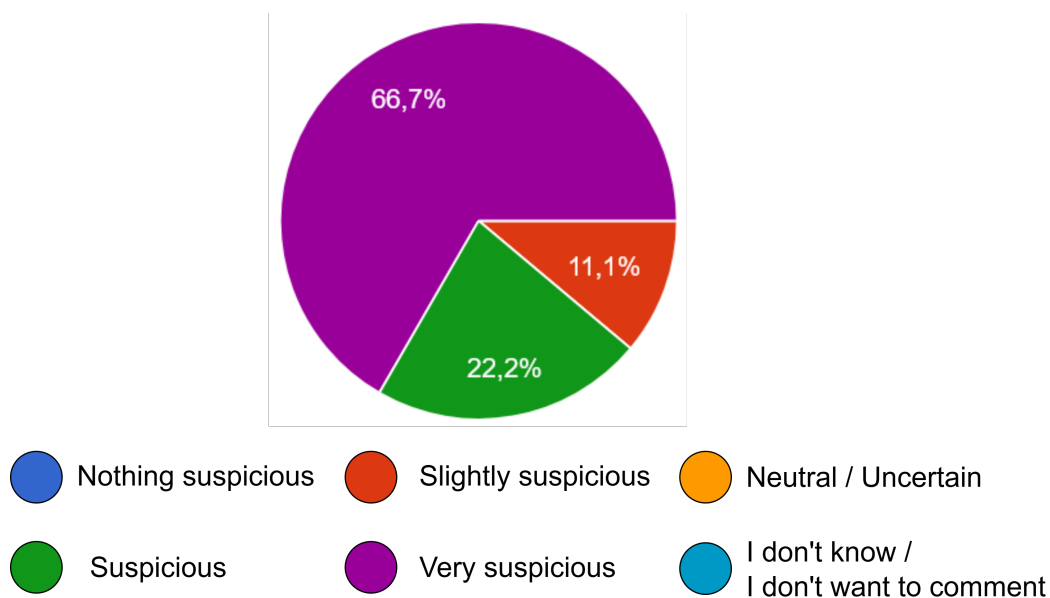


Figure 6.24: Auditor Perceived Degree of Suspicion (Case 6)

Figure 6.25 illustrates the priority assigned for further investigation. A majority of respondents (55.6%) indicated that the case should be investigated with high priority, while 44.4% recommended maximum priority. No auditor suggested medium or low pri-

ority, nor refraining from investigation. This distribution demonstrates that suspicion translated directly into operational urgency, particularly influenced by the contract value combined with the waiver modality (dispensa).

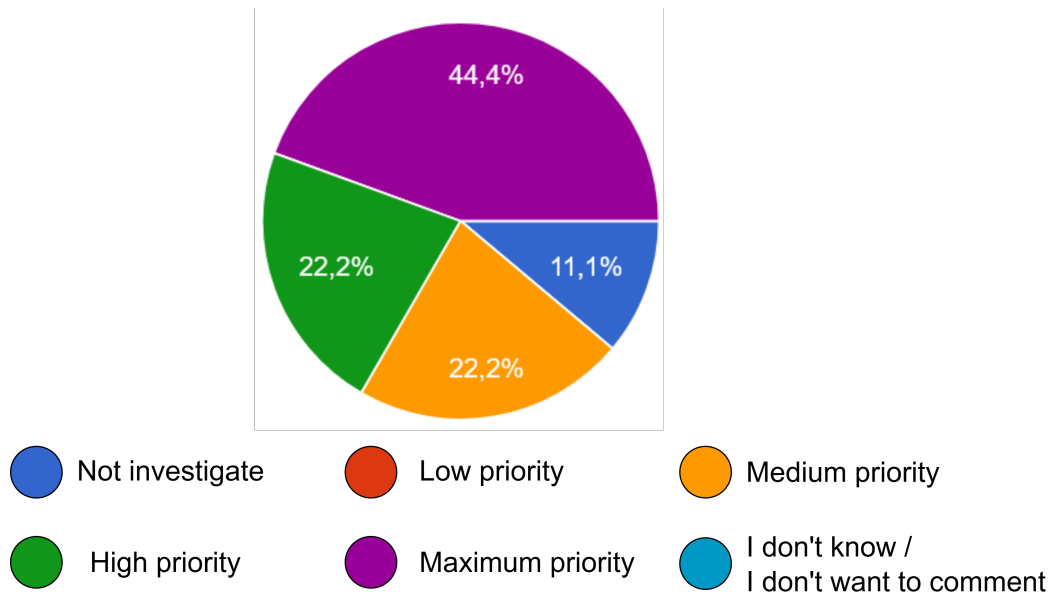


Figure 6.25: Investigation Priority Assessment by Auditors (Case 6)

Figure 6.26 presents the perceived relevance of each activated red flag. Political donation indicators (party and candidate donations) were predominantly rated as high or extreme relevance. The flag concerning high participation in government contracts also received strong relevance ratings, suggesting concerns about potential concentration or preferential access. The capital social below contract value showed slightly more dispersion, being interpreted as indicative but not necessarily determinative in isolation. Overall, auditors appear to attribute higher weight to the political exposure and structural dependency on public contracts than to financial proportionality alone.

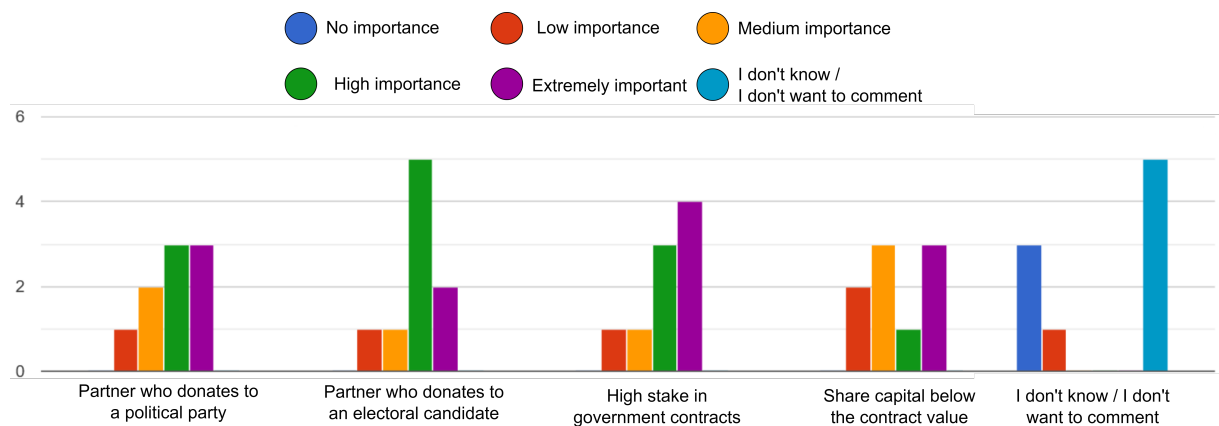


Figure 6.26: Perceived Relevance of Activated Red Flags (Case 6)

Finally, Figure 6.27 reports auditor agreement with the automated classification of the case as high risk. A majority (44.4%) expressed total agreement, 22.2% indicated partial agreement, 22.2% were neutral, and 11.1% expressed partial disagreement. No respondent expressed total disagreement. Compared to earlier cases, this distribution reflects a more nuanced alignment between professional judgment and model output, suggesting that while the classification is broadly supported, auditors contextualize their agreement based on additional elements such as materiality, procurement modality, and the intrinsic nature of the contract.

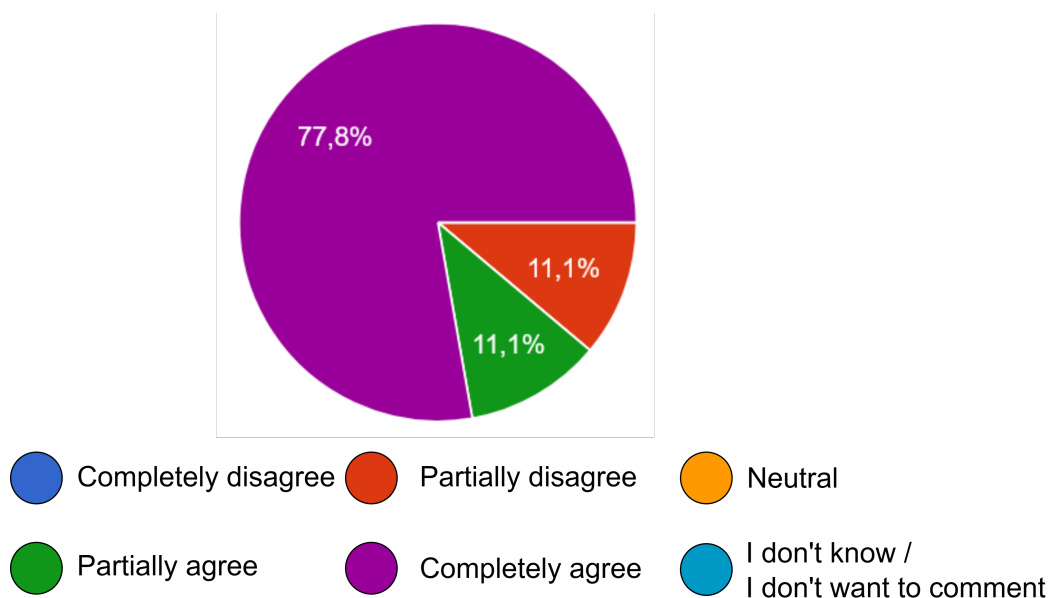


Figure 6.27: Auditor Agreement with Model Classification (Case 6)

The qualitative comments reinforce this interpretative dimension. Auditors emphasized that the identified red flags constitute important indicators but not conclusive evidence of fraud. Some respondents highlighted that additional elements — such as evidence of bid rigging, overpricing, or market restriction — would strengthen the suspicion. Others pointed out that the combination of waiver modality and contract value was more decisive than individual flags alone, and that materiality relative to the contracting entity's budget should be considered. These remarks illustrate the contextual reasoning applied by professionals when translating analytical signals into oversight decisions.

- These are just indications. If there were other indications, such as bid rigging, overpricing, or overbilling, then it would gain more weight.
- The very nature of the contract is already noteworthy. All these red flags are important indications of fraud.

- I would investigate by the combination of exemption x value, not exactly by the flags, and always considering the context of the scale of values executed by the agency.

6.2.3 Ethical Evaluation

In addition to the technical and institutional assessments of data sources and risk indicators, a complementary evaluation was conducted to examine ethical dimensions associated with the application of AI in fraud detection within public procurement. This stage aimed to assess the perceived relevance of fundamental ethical principles in the design and deployment of AI-based decision-support systems. The evaluation instrument was grounded in the European Commission’s document *Ethics Guidelines for Trustworthy AI*, which establishes core requirements to ensure that AI systems operate in a transparent, accountable, and governance-aligned manner.

Due to practical constraints, this stage of the evaluation was conducted with a single respondent, an experienced chief public auditor with extensive expertise in procurement oversight. While the limited number of participants restricts the generalizability of findings, the seniority and institutional experience of the respondent provide qualified insight into how ethical considerations are perceived within high-level audit practice. The instrument consisted of five statements corresponding to key ethical dimensions derived from the European guidelines. The participant was asked to indicate the degree of agreement with each statement on a five-point Likert scale ranging from “strongly disagree” to “strongly agree,” and to provide qualitative comments justifying the chosen responses. Participation was voluntary, and responses were collected anonymously in accordance with an informed consent protocol.

The responses reveal a nuanced and context sensitive understanding of ethical requirements in AI supported fraud detection. Regarding transparency and explainability, the respondent expressed agreement, while emphasizing that complete traceability of highly complex AI models may be technically infeasible. Instead, what was considered ethically reasonable was the provision of structured explanations detailing the main reasoning chain, key procedures that led to anomaly detection, and the data sources employed. This position reflects a pragmatic interpretation of explainability, prioritizing actionable justification over exhaustive cognitive traceability.

On the need for case-specific justification and interpretability of AI outputs, the respondent expressed total agreement, highlighting that ethical adequacy requires detailed

explanations tailored to each concrete situation. The importance of enabling verification, contestation, and effective oversight was strongly emphasized, reinforcing the alignment between AI transparency and procedural guarantees in public administration.

Concerning automated decision making and potential risks associated with AI autonomy, the respondent adopted a neutral position, noting uncertainty regarding the practical implications of fully automated systems in public procurement. The auditor emphasized that, in practice, fraud detection systems, whether AI-based or not, generate alerts that must undergo rigorous human verification processes, including procedural safeguards such as adversarial review and due process. This reasoning suggests that existing institutional mechanisms mitigate risks associated with automation, provided that AI systems are deployed strictly as decision-support tools rather than autonomous decision-makers.

Regarding human oversight and continuous interaction between analysts and AI systems, the respondent expressed total agreement, stressing that AI should function as an auxiliary instrument within a broader human controlled process. The comments highlighted that regulatory changes, jurisprudential developments, evolving fraud schemes, and institutional reforms require constant adaptation of detection models, making sustained human supervision indispensable.

Finally, in relation to governance and institutional control mechanisms, the respondent adopted a neutral stance, indicating uncertainty about the specific formulation of the question. Nevertheless, the qualitative comments underscored the importance of centralized oversight, coordination, and efficiency in the Brazilian procurement monitoring ecosystem. The respondent emphasized that transparency mechanisms such as the PNCP enable systemic supervision and that dispersed and fragmented control arrangements may undermine institutional efficiency. This perspective reinforces the relevance of governance architecture in shaping ethical AI deployment, even when conceptual interpretations of specific constructs may vary.

Overall, although limited to a single expert perspective, the ethical evaluation highlights a consistent emphasis on transparency, human oversight, proportionality, and institutional governance as essential components of trustworthy AI in public procurement. The findings reinforce the positioning of the referenced model as a decision-support artifact that must remain embedded within human-controlled oversight structures, ensuring that automated risk signals are interpreted, contextualized, and validated within established legal and procedural safeguards.

6.3 Discussion of Results, Design Implications, and Limitations

The results presented in this chapter provide a multidimensional assessment of the referenced model, combining (i) the expert-based evaluation of data sources and red flags, (ii) the technical evaluation of anonymized procurement cases, and (iii) the ethical appraisal of AI-related design principles. Taken together, these findings allow a structured reflection on the institutional plausibility, interpretative robustness, and governance alignment of the proposed artifact.

From the perspective of data sources, the expert evaluation demonstrated broad agreement regarding the relevance of core public datasets. Auditors consistently emphasized the importance of cross-referencing heterogeneous databases as a necessary condition for meaningful fraud detection. At the same time, qualitative comments revealed practical concerns regarding data accessibility, file usability, update frequency, and structural fragmentation. These findings reinforce a key design implication of the referenced model: fraud detection effectiveness is not solely dependent on indicator design, but fundamentally on the quality, interoperability, and operational accessibility of underlying open government data infrastructures.

Regarding the red flags, the evaluation revealed strong convergence between the proposed indicators and auditors' professional experience. Most red flags were considered relevant and operationally meaningful, particularly those associated with political exposure, sanction records, incompatibilities in corporate registration data, and disproportionate contractual patterns. However, auditors consistently stressed that red flags should be interpreted as indicative signals rather than conclusive evidence. This reinforces a central design principle of the model: red flags must function as risk signals embedded within a decision-support logic, not as automated adjudicative mechanisms. The qualitative responses highlight that convergence, accumulation, and contextualization of multiple indicators are essential for translating analytical signals into legitimate oversight actions.

The case-based technical evaluation further illuminates how professional judgment interacts with automated classifications. In cases involving strong structural inconsistencies or sanction-related indicators, alignment between auditors and the model was high. Conversely, in cases characterized by low materiality, ambiguous political signals, or context-dependent interpretations, agreement levels were more heterogeneous. These results reveal an important boundary condition: while the referenced model effectively

captures structural and compliance-related risk signals, the translation of such signals into investigative prioritization remains mediated by proportionality, materiality, and contextual reasoning. This confirms the socio-technical positioning of the artifact, in which automated outputs require professional interpretation rather than replacing institutional discretion.

The ethical evaluation, albeit conducted with a single senior auditor, provides additional insight into governance and transparency dimensions. The responses emphasized the necessity of explainability at a level sufficient for procedural justification, rather than complete cognitive traceability of complex models. Strong agreement with human oversight requirements reinforces the decision-support orientation of the referenced model, aligning it with principles of non-automation of final decisions. The responses regarding automated decision-making and governance structures suggest that ethical adequacy is perceived not merely as a technical feature of AI systems, but as a function of institutional embedding, procedural safeguards, and centralized oversight architectures.

Taken together, these findings generate several design implications. First, the referenced model should incorporate explicit mechanisms for contextual calibration, allowing materiality and institutional scale to inform risk prioritization. Second, provenance and traceability mechanisms become critical to support explainability expectations articulated by auditors. Third, red flag activation logic should emphasize cumulative reasoning rather than isolated signal triggering, reflecting professional interpretative patterns. Finally, the artifact must remain structurally positioned as a human-centered analytical instrument, preserving procedural guarantees and institutional accountability.

Despite these contributions, important limitations must be acknowledged. The expert-based evaluation of data sources and red flags was conducted within a Brazilian institutional context, which may limit generalizability to other procurement ecosystems. The case-based technical evaluation involved nine auditors and six cases, providing depth but not statistical representativeness. The ethical evaluation relied on a single senior auditor, offering qualified insight but lacking plurality of perspectives. Furthermore, the empirical validation does not constitute large-scale longitudinal testing of predictive performance across extensive procurement datasets. The referenced model was evaluated primarily in terms of institutional plausibility, interpretability, and contextual adequacy, rather than exhaustive predictive benchmarking.

Accordingly, the results should be interpreted as evidence of socio-technical alignment and design adequacy within the defined research scope, rather than as definitive proof of

universal effectiveness. Future research may expand the evaluation to larger auditor samples, cross-country institutional contexts, extended datasets, and experimental calibration of prioritization thresholds. Nonetheless, within the boundaries of this thesis, the findings demonstrate that the referenced model achieves meaningful convergence with professional judgment, supports ethically grounded AI integration, and operates coherently as a structured decision-support artifact for fraud risk analysis in public procurement.

Chapter 7

Analytics Capability and Socio-Technical Conditions

This chapter examines how different procurement OGD ecosystems provide conditions for fraud risk analysis and AI-supported oversight in PP. More specifically, the chapter investigates the relationship between data quality and broader socio-technical conditions associated with analytics capability by comparing procurement OGD environments from Brazil, the Netherlands, and the European Union. This stage of the research was developed during the PhD exchange period conducted at Delft University of Technology (TU Delft), where the author had the opportunity to closely examine the Dutch and European procurement data ecosystems and observe substantial differences in how procurement data infrastructures are organized, documented, integrated, and made available for analytical reuse when compared to the Brazilian context. To achieve this, the study combines a quantitative assessment of data quality with a qualitative analysis focused on organizational, institutional, legal, and cultural dimensions that influence the analytical capability of procurement data ecosystems.

The relevance of this analysis to the proposed reference model lies in the fact that its effective instantiation depends on the characteristics of the environment in which it is applied. While the reference model defines the components and relationships required to transform procurement data into interpretable fraud risk information and support auditing activities, the extent to which these components can be operationalized is conditioned by the analytics capability of the surrounding data ecosystem. In this sense, analytics capability is not conceived as an additional component of the reference model, but as a contextual condition for its instantiation. Examining data quality together with organizational, institutional, legal, and cultural conditions therefore provides a means to identify factors that may enable or constrain the operationalization of the model across

different procurement environments, contributing to an understanding of its applicability and adaptability beyond the Brazilian context.

7.1 Comparative Research Design

The research design adopted combines quantitative and qualitative analytical approaches to compare procurement OGD ecosystems from Brazil, the Netherlands, and the European Union, investigating how data quality dimensions together with socio-technical conditions contribute to analytics capability and support data-driven applications in public procurement. The quantitative stage is based on the data quality assessment framework proposed by (VETRÒ et al., 2016), enabling the systematic evaluation of procurement-related datasets through measurable dimensions such as traceability, currentness, expiration, completeness, compliance, understandability, and accuracy. Complementarily, the qualitative stage is grounded in the socio-technical perspectives proposed by (LNENICKA et al., 2024), (KASSEN, 2018), and (ALTAYAR, 2018), supporting the interpretation of how legal, organizational, institutional, and cultural conditions influence the analytics capability of procurement OGD ecosystems.

The selection of Brazil, the Netherlands, and the European Union was motivated by their distinct positions and characteristics within the context of procurement-related OGD ecosystems. Brazil was selected due to its recent international recognition regarding open data initiatives ¹ and the high availability and granularity of procurement-related datasets, providing a relevant context for analyzing ecosystems characterized by broader transparency and interoperability conditions. The European Union was selected because of its historical role as one of the major global references in OGD policies and standardization initiatives, particularly through supranational governance mechanisms and procurement transparency frameworks such as TED ². The Netherlands was selected both because of its prominent positions in the implementation of open government data initiatives (SAFAROV, 2019) and because it presents institutional, cultural, and governance characteristics substantially different from the Brazilian case, particularly regarding data disclosure practices, transparency culture, privacy regulations, and administrative coordination. Together, these contexts provide a suitable comparative setting for examining how different socio-technical and institutional conditions influence the analytics capability of procurement OGD ecosystems.

¹<https://www.gov.br/secom/pt-br/acompanhe-a-secom/noticias/2026/03/brasil-alcanca-melhor-resultado-da-historia-em-ranking-da-ocde-sobre-dados-abertos>

²<https://ted.europa.eu/en/>

Figure 7.1 summarizes the research design adopted in this study. The methodological flow begins with the selection of procurement OGD portals from Brazil, the Netherlands, and the European Union, followed by the data collection stage and a narrative literature review aimed at identifying the theoretical and methodological foundations supporting both the quantitative and qualitative analyses. From this review, the study selects the data quality assessment framework, for the quantitative stage, as well as the socio-technical perspectives to support the qualitative comparative analysis.

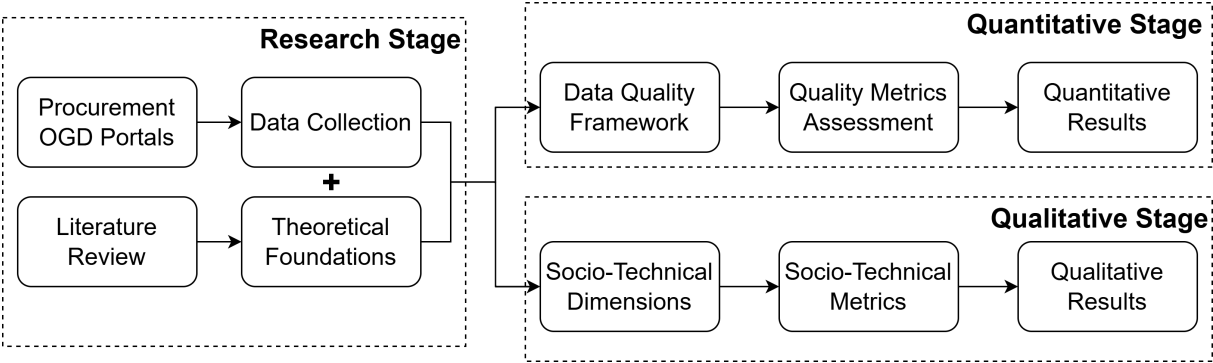


Figure 7.1: Research Design for Analytics Capability and Data Quality Assessment

7.2 Quantitative Assessment of Data Quality

The quantitative assessment focuses on evaluating the quality characteristics of procurement-related OGD datasets through a set of objective and measurable indicators applied at the dataset level. This approach enables a more granular evaluation of the data itself, rather than broader platform-level characteristics, supporting the systematic comparison of procurement OGD ecosystems across different institutional contexts. The assessment is centered on intrinsic data quality dimensions that can be directly observed in the datasets, independently of specific user perceptions or application scenarios. These dimensions include traceability, currentness, expiration, completeness, compliance, understandability, and accuracy, each representing distinct aspects associated with the reliability, structure, and usability of procurement-related OGD.

7.2.1 Quantitative Assessment: Data Quality Framework

Each dimension is defined through one or more quantitative metrics, which translate abstract quality concepts into measurable indicators. Table 7.1 presents the structure of the data quality assessment framework, detailing the relationship between each dimension,

its corresponding metrics, and the formal definitions used for their computation. For each metric, the table specifies the level of analysis (e.g., cell, row, column, or dataset), a concise description of its purpose, and its mathematical formulation, including both the raw computation and the normalization function applied to standardize the results. In addition, the table explicitly reports the scale associated with each metric, capturing the original range of values prior to normalization. This structured representation not only clarifies how each data quality dimension is quantified, but also highlights the heterogeneity of the metrics in terms of computational logic, ranging from simple proportions to temporal functions and piecewise normalization rules.

Table 7.1: Data Quality Dimensions and Metrics

Dimension	Metric	Level	Description	Formula	Normalization	Scale
Traceability	Track of creation	Dataset	Verifies the availability of metadata describing the origin and creation of the dataset	$tc = 2s + ds$	$tcn = \frac{tc}{2}$	$[0, 3]$
	Track of updates	Dataset	Verifies the availability of metadata describing dataset updates and versioning	$tu = lu + du$	$tun = \frac{tu}{2}$	$[0, 2]$
Currentness	Percentage of current rows	Row/Cell	Measures the proportion of records that are temporally up-to-date	$pcr = (1 - \frac{ncr}{nr}) \times 100$	$pcrn = \frac{pcr}{100}$	$[0\%, 100\%]$
	Delay in publication	Dataset	Measures the delay between data availability and publication	$da = ed + 1$ $dp = 1 - (\frac{ed - sd}{2d - sd})$	$dpm = dp$	$(-\infty, 1]$
Expiration	Delay after expiration	Dataset	Measures the delay between dataset expiration and its update/replacement	$dac = 1 - (\frac{ed - sd}{2d - sd})$	$ifdae \leq 0, daen = 0$ $ifdae \leq 1, daen = rs$ $ifdae > 1, daen = 1$	$(-\infty, +\infty)$
Completeness	Percentage of complete cells	Cell	Measures the proportion of non-empty and valid cells	$ncl = nr * nc$ $pcc = (1 - \frac{ncl}{nc}) \times 100$	$pcca = \frac{pcc}{100}$	$[0\%, 100\%]$
	Percentage of complete rows	Row	Measures the proportion of rows without missing values	$pcpr = (1 - \frac{nrc}{nr}) \times 100$	$pcpra = \frac{pcpr}{100}$	$[0\%, 100\%]$
Compliance	Percentage of standardized columns	Column	Measures adherence to domain-specific standards (e.g., formats, identifiers)	$psc = \frac{ncs}{nc} \times 100$	$pscn = \frac{psc}{100}$	$[0\%, 100\%]$
	eGMS compliance	Dataset	Measures compliance with core metadata standards	$egmsc = s + dc + c + t + 0.2(d + id + pb + cv + l)$	$egmscn = \frac{egmsc}{5}$	$[0-5]$
	Five-star open data	Dataset	Measures level of openness according to the five-star model	-	$fsodn = \frac{fsod}{5}$	$[0, 5]$
Understandability	Percentage of columns with metadata	Column	Measures the availability of descriptive metadata for dataset attributes	$pcm = \frac{um}{uc} \times 100$	$pcmn = \frac{pcm}{100}$	$[0, 100]$
	Percentage of columns in comprehensible format	Column	Measures whether data is represented in interpretable and machine-readable formats	$pcuf = \frac{ucf}{uc} \times 100$	$pcufa = \frac{pcuf}{100}$	$[0\%, 100\%]$
Accuracy	Percentage of accurate cells	Cell	Measures the proportion of values that conform to expected domains or formats	$pac = (1 - \frac{ncv}{nc}) \times 100$	$paca = \frac{pac}{100}$	$[0\%, 100\%]$
	Accuracy in aggregation	Cell/Dataset	Measures consistency between aggregated values and expected totals	$e = \sum_{i=1}^n davi - oavi $ $ea = 1 - (\frac{e}{n})$	$ifea \leq 0, ean = 0$ $elifea \leq 0.9, ean = 0.25 * ea$ $elifea \leq 0.95, ean = 0.5 * ea$ $elifea \leq 0.999, ean = 0.75 * ea$	$(-\infty, 1]$

The variables used in the formulation of the data quality metrics are defined according to the structure and metadata of each dataset. In the context of traceability, s denotes the presence of source information, while dc represents the availability of the dataset creation date. For update-related metadata, lu corresponds to the existence of a list of updates and du to the availability of update timestamps. Temporal aspects of the data are captured through variables such as ncr , representing the number of non-current rows, and nr , the total number of rows. Additional temporal variables include da , the date of information availability; dp , the date of publication; sd and ed , the start and end dates of the reference period covered by the dataset; cd , the current date; and ed , also used to denote the expiration date of the dataset.

For completeness-related metrics, nc denotes the number of columns, ic the number

of incomplete cells, nir the number of incomplete rows, and ncl the total number of cells in the dataset, computed as the product of rows and columns. In the compliance dimension, ns represents the number of columns associated with standards, while nsc denotes the number of standardized columns. Metadata-related variables include c (category), t (title), d (description), id (identifier), pb (publisher), cv (coverage), and l (language), which are used to assess compliance with metadata standards.

In terms of understandability, ncm represents the number of columns with associated metadata, and $ncuf$ the number of columns expressed in a comprehensible format. Accuracy is measured using nce , the number of cells containing errors, and ncl , the total number of cells. Finally, for aggregation accuracy, e denotes the total aggregation error, computed as the sum of absolute differences between the dataset aggregation values dav_i and the corresponding reference aggregation values oav_i , while s represents the scale used to normalize this error.

The empirical analysis is conducted based on official OGD portals that provide access to public procurement data in the selected contexts. In Brazil, the primary source is the *Portal Nacional de Contratações Públicas* (PNCP), which serves as the central platform for the publication and integration of procurement-related information across different levels of government. In the Netherlands, procurement data is accessed through *TenderNed*, the official national platform that supports the publication and management of public tenders and contract notices. At the European level, the analysis relies on *Tenders Electronic Daily* (TED), the official online version of the Supplement to the Official Journal of the European Union, which aggregates procurement notices from member states. These portals were selected due to their institutional relevance, official status, and role as primary channels for the disclosure of procurement-related data within their respective jurisdictions.

The empirical analysis is conducted based on official OGD portals that provide access to public procurement data in the selected contexts. In Brazil, the primary source is the *Portal Nacional de Contratações Públicas* (PNCP) ³, which serves as the central platform for the publication and integration of procurement-related information across different levels of government. In the Netherlands, procurement data is accessed through *TenderNed* ⁴, the official national platform that supports the publication and management of public tenders and contract notices. At the European level, the analysis relies

³<https://www.gov.br/pncp/pt-br>

⁴<https://www.tenderned.nl/cms/nl>

on *Tenders Electronic Daily* (TED) ⁵, the official online version of the Supplement to the Official Journal of the European Union, which aggregates procurement notices from member states. These portals were selected due to their institutional relevance, official status, and role as primary channels for the disclosure of procurement-related data within their respective jurisdictions.

The application of the framework follows a structured analytical procedure. First, datasets are identified and selected from each portal based on their relevance to public procurement. Second, the selected datasets are preprocessed to ensure structural consistency, including schema inspection and data cleaning when necessary. Third, the data quality metrics defined in Table 7.1 are computed for each dataset, either automatically or through manual inspection depending on the nature of the metric. Fourth, all metric values are normalized to a common scale to allow comparability across datasets with different structures. Finally, the resulting indicators are analyzed comparatively across the three contexts (Brazil, Netherlands, and European Union) in order to identify patterns, differences, and structural characteristics in the data quality of procurement-related OGD.

7.2.2 Comparative Quantitative Results

This subsection presents the results of the quantitative data quality assessment conducted across the selected OGD portals for public procurement in Brazil, the Netherlands, and the European Union. Using the framework described in Section 7.2.1, datasets were evaluated along multiple data quality dimensions, generating a set of comparable indicators for each context. The results are organized through a comparative analysis detailing the performance of each ecosystem across the defined quality metrics, highlighting similarities and differences related to the dimensions.

In order to ensure comparability across the three contexts, the analysis was restricted to the most recent period for which data was available across the Brazilian, Dutch, and European Union portals. While data for Brazil and the Netherlands was available for the year 2024, the European Union dataset was only available up to 2023, which represents the latest complete reporting period at the time of data collection. This temporal alignment reduces potential biases arising from differences in data availability and update cycles across the platforms, while ensuring that each context is represented by its most recent data. Table 7.2 presents a comparative overview of key descriptive statistics for the analyzed OGD portals, including the number of procurement records, number of

⁵<https://data.europa.eu/data/datasets/ted-csv?locale=en>

suppliers, total contract value, as well as average and median contract values. These indicators provide an initial characterization of each dataset, capturing differences in scale, economic volume, and distribution of procurement activities across the three contexts. Such variations are relevant for contextualizing the subsequent data quality assessment, as they reflect underlying structural and institutional factors that shape the availability and organization of procurement data.

Table 7.2: Comparative Descriptive Statistics of Datasets in Brazil, the Netherlands, and the EU

Portal	Brazil	Netherlands	European Union
Number of contracts	428.926	34.060	305.470
Number of suppliers	199.580	6914	244.054
Total contract value (EUR)	899.329.707.528	47.572.981.777	–
Average contract value (EUR)	2.096.701	1.396.740	–
Average supplier value (EUR)	4.506.111	6.880.674	–

The descriptive statistics presented in Table 7.2 reveal clear structural differences across the three datasets, while also highlighting important data quality constraints that directly affect the interpretation of value-based indicators. In terms of scale, Brazil exhibits the largest number of contracts (428,926), followed by the European Union (305,470) and the Netherlands (34,060), suggesting a broader coverage and higher level of granularity in the Brazilian dataset. A similar pattern is observed for the number of suppliers, although the ratio between contracts and suppliers differs across contexts, indicating variations in market concentration and participation dynamics. For instance, the Netherlands shows a relatively smaller supplier base compared to the number of contracts, which is reflected in a higher average supplier value, suggesting a more concentrated supplier structure.

When analyzing financial indicators, Brazil presents a substantially higher total contract value (approximately €899 billion) compared to the Netherlands (€47.5 billion), which is consistent with its larger scale. However, average contract values are relatively comparable (€2.09M in Brazil versus €1.39M in the Netherlands), indicating that, despite differences in volume, the typical contract size remains within a similar order of magnitude. The average supplier value further reinforces structural differences: while Brazil distributes value across a larger number of suppliers, the Netherlands concentrates higher value per supplier, which may indicate differences in procurement practices, market structure, or aggregation levels in the data.

In contrast, value-based indicators for the European Union dataset are reported as –,

which is not merely a limitation of the current analysis but reflects a well-documented issue in the TED data. As highlighted in the official documentation, contract values in notices suffer from multiple data quality problems, including a high proportion of missing values in some Member States and the presence of nonsensical or erroneous values. Additionally, a critical structural issue arises from framework agreements, where some countries report both the maximum value of the framework and the individual contracts awarded under it. Since the current TED data model does not allow distinguishing between these cases, both the total value and even the number of contract award notices can be artificially inflated.

Given these limitations, the European Commission itself recommends prioritizing count-based indicators over value-based ones for comparative analyses, as they are less sensitive to inconsistencies and duplication effects. In line with this guidance, the absence of EU value indicators in Table 7.2 reflects a methodological choice aimed at preserving analytical validity. Overall, these patterns reinforce a central insight of this study: while data availability is a necessary condition for analysis, it is the underlying data quality and structural consistency that ultimately determine the reliability and comparability of derived indicators across different procurement ecosystems.

The framework was systematically applied to each dataset, generating a set of quantitative indicators across the defined data quality dimensions. These results enable a structured comparison of the datasets, allowing differences and similarities to be identified in terms of their intrinsic characteristics. Table 7.3 and Figure 7.2 summarizes the outcomes of this assessment, providing a consolidated view of the data quality metrics computed for each context.

Table 7.3: Comparative Data Quality Assessment of Public Procurement OGD Portals

Dimension	Metric	BR	NL	EU	Norm-BR	Norm-NL	Norm-EU
Traceability	1. Track of creation	1	0	1	0.33	0	0.33
	2. Track of updates	2	0	0	1	0	0
Currentness	3. Percentage of current rows	100	100	100	1	1	1
	4. Delay in publication	0.935	0.6415	0.8362	0.94	0.64	0.84
Expiration	5. Delay after expiration	–	–	–	–	–	–
Completeness	6. Percentage of complete cells	67.92	50.25	72.89	0.68	0.5	0.73
	7. Percentage of complete rows	0	0	0	0	0	0
Compliance	8. Percentage of standardized columns	100	100	100	1	1	1
	9. eGMS compliance	4.8	2.8	5	0.96	0.56	1
	10. Five-star open data	3	3	4	0.60	0.60	1
Understandability	11. Percentage of columns with metadata	100	100	100	1	1	1
	12. Percentage of columns in comprehensible format	100	100	100	1	1	1
Accuracy	13. Percentage of accurate cells	97.41	96.86	100	0.97	0.97	1
	14. Accuracy in aggregation	–	–	–	–	–	–

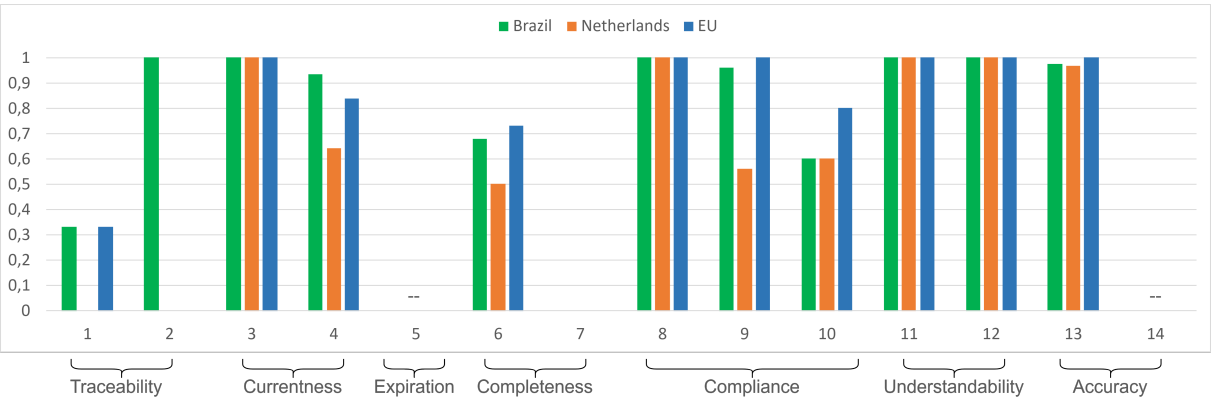


Figure 7.2: Histogram from Comparative Data Quality Assessment of Public Procurement OGD Portals

The Brazilian dataset presents full coverage in the currentness dimension, with 100% of rows aligned with the reference period and a normalized delay in publication score of 0.94. In terms of traceability, the dataset achieves a score of 1 for track of creation and 2 for track of updates, indicating the presence of some mechanisms related to data origin and update information, although not explicitly structured. The expiration dimension could not be assessed due to the absence of relevant metadata.

Regarding completeness, the dataset shows 67.92% of complete cells, while the percentage of complete rows is 0%, as all records contain at least one missing value. In the compliance dimension, all columns are standardized (100%), and the dataset achieves an eGMS compliance score of 4.8 (normalized to 0.96). The dataset is classified as three-star open data. In terms of understandability, all columns are associated with metadata and

are presented in a comprehensible format. Finally, the dataset reaches 97.41% in the percentage of accurate cells. The accuracy in aggregation metric was not applied, as the dataset contains only granular data and does not provide aggregated values that could be compared against detailed records.

The dataset from the Netherlands shows a score of 0 for both track of creation and track of updates in the traceability dimension, indicating the absence of identifiable metadata for these aspects. The currentness dimension is fully satisfied, with 100% of rows aligned with the reference period and a normalized delay in publication score of 0.64. As in the Brazilian case, the expiration dimension could not be evaluated.

In terms of completeness, the dataset presents 50.25% of complete cells and 0% of complete rows. All columns are standardized (100%), and the eGMS compliance score is 2.8 (normalized to 0.56). The dataset is classified as three-star open data. For understandability, all columns are associated with metadata and presented in a comprehensible format. The percentage of accurate cells is 96.86%. The accuracy in aggregation metric was not applied, as only granular data is available and no aggregated values are provided for consistency verification.

The European Union dataset achieves a score of 1 for track of creation and 0 for track of updates in the traceability dimension. The currentness dimension is fully satisfied, with 100% of rows aligned with the reference period and a normalized delay in publication score of 0.84. The expiration dimension could not be assessed due to the absence of corresponding metadata.

In the completeness dimension, the dataset shows 72.89% of complete cells and 0% of complete rows. All columns are standardized (100%), and the dataset achieves an eGMS compliance score of 5 (normalized to 1.00). It is classified as five-star open data. In terms of understandability, all columns are associated with metadata and presented in a comprehensible format. The percentage of accurate cells is 100%. The accuracy in aggregation metric was not applied, as the dataset consists exclusively of granular data and does not include aggregated information for comparison.

From a comparative perspective, the results presented in Table 7.3 reveal differences across the three OGD ecosystems that go beyond individual metrics and highlight structural characteristics of each context. One notable aspect relates to language availability. Among the analyzed portals, only the European Union dataset provides support for multiple languages, reflecting its inherently multinational scope. In contrast, both the Brazilian and Dutch portals are limited to a single language, which may impose barriers

for broader accessibility and reuse by international stakeholders. It is also important to note that some metrics were classified as not applicable – across all analyzed datasets due to structural limitations in the available data. In particular, the delay after expiration metric could not be calculated because none of the datasets provide metadata related to expiration dates or validity periods. Similarly, the accuracy in aggregation metric could not be assessed because the analyzed datasets consist exclusively of granular records and do not include aggregated panels or summarized values that could be compared against detailed data for consistency verification.

When comparing Brazil and the Netherlands, the Brazilian dataset consistently presents higher values across multiple dimensions, particularly in traceability, delay in publication, completeness, and compliance. While both contexts exhibit similar behavior in dimensions such as currentness, standardization, understandability, and accuracy, the Brazilian dataset demonstrates more favorable results in terms of data availability and structural completeness. These differences are directly reflected in the normalized scores, where Brazil outperforms the Netherlands in most of the evaluated metrics.

The European Union dataset achieves the highest overall scores according to the adopted framework, particularly in compliance and completeness, as well as in the five-star open data classification. However, it is important to note that this classification is strongly influenced by the adoption of RDF and linked data principles. While this results in a higher formal score, the presence of RDF alone does not necessarily translate into improved analytical usability. In practice, aspects such as documentation clarity and data dictionary interpretability remain relevant factors that are not fully captured by the five-star model. This observation provides an initial indication that higher scores in standardized openness metrics may not directly correspond to better conditions for analytical use, a point that is further explored in the subsequent discussion section.

7.3 Socio-technical Qualitative Analysis

Complementing the quantitative data quality assessment, this study also adopts a qualitative comparative analysis aimed at interpreting how socio-technical conditions influence the analytics capability of procurement OGD ecosystems. While the quantitative stage provides measurable indicators regarding intrinsic data quality dimensions, it does not fully explain the observed differences in analytical usability across the analyzed contexts. Therefore, the qualitative assessment seeks to contextualize these findings by examining

how legal and regulatory environments, institutional structures and organizational arrangements, and cultural orientations shape the characteristics and analytics capability of procurement-related OGD.

7.3.1 Qualitative Assessment: Socio-Technical Perspectives

The qualitative comparative assessment was guided by a set of analytical dimensions derived from the theoretical perspectives proposed by (LNENICKA et al., 2024), (KASSEN, 2018), and (ALTAYAR, 2018). These dimensions support the interpretation of how legal, organizational/institutional, cultural conditions influence the analytics capability of procurement OGD ecosystems beyond purely technical data quality characteristics. Table 7.4 summarizes the analytical dimensions adopted in this stage of the study and their respective analytical focus within the comparative assessment.

Table 7.4: Analytical Dimensions in Qualitative Assessment

Reference	Dimension	Qualitative Indicator	Analytical Focus in This Study
(LNENICKA et al., 2024)	Organizational/Institutional	Data Interoperability	Evaluation of the potential for cross-dataset linkage, interoperability, and integration across domains.
(LNENICKA et al., 2024)	Organizational/Institutional	Value-Adding	Evaluation of the contribution of public data ecosystem elements, relationships, and processes toward value creation through data use, reuse, sharing, and analytical purposes.
(LNENICKA et al., 2024)	Cultural	Collaboration Culture	Evaluation of the extent to which collaboration, participation, co-creation, and trust among ecosystem stakeholders support transparency, data sharing, interoperability, and value creation within the public data ecosystem.
(KASSEN, 2018)	Cultural	Self-Governance	Evaluation of the extent to which traditions of local autonomy and self-governance support OGD initiatives.
(KASSEN, 2018)	Legal/Regulatory	Policy Standardization	Evaluation of the existence of standardized policies, implementation mechanisms, and governance procedures across jurisdictions.
(KASSEN, 2018)	Organizational/Institutional	Ecosystem Governance	Evaluation of the capacity of governmental institutions and open data platforms to coordinate, maintain, standardize, and sustain the operation, quality, and evolution of the OGD ecosystem.
(ALTAYAR, 2018)	Legal/Regulatory	Regulatory Governance	Examination of how legal frameworks (such as GDPR, LGPD, etc) influence data disclosure and reuse.
(ALTAYAR, 2018)	Culture	Openness Culture	Evaluation of cultural orientations toward openness, disclosure, and data protection.
(ALTAYAR, 2018)	Organizational/Institutional	Institutional Drivers	Examination of pressures from oversight bodies, legislation, and society influencing OGD adoption and governance.

Together, these analytical dimensions provide a structured basis for interpreting OGD ecosystems across the analyzed context. Rather than evaluating data quality exclusively through intrinsic technical metrics, this qualitative assessment enables the study to examine how broader socio-technical conditions influence the analytics capability of procurement-related OGD. By integrating these dimensions with the quantitative findings obtained in the previous stage, the study seeks to develop a more comprehensive

understanding of how different characteristics shape the potential of OGD to support analytics capability in public procurement.

7.3.2 Comparative Qualitative Results

This subsection moves beyond the quantitative assessment of data quality to examine the broader socio-technical conditions that shape the analytical usability of OGD in public procurement. While the results presented in the previous section provide a structured evaluation of datasets across Brazil, the Netherlands, and the European Union, they do not fully explain the observed differences in their potential to support analytics capability. To address this gap, this section adopts a comparative socio-technical perspective focused on how legal, cultural, institutional, and organizational conditions influence the transformation of data quality into analytics capability within procurement OGD ecosystems. The discussion is grounded in the complementary perspectives proposed by (LNENICKA et al., 2024), (KASSEN, 2018), and (ALTAYAR, 2018). Together, these studies support the interpretation of procurement OGD ecosystems beyond purely technical data quality dimensions, emphasizing aspects related to Data Interoperability, Value-Adding, Collaboration Culture, Self-Governance, Policy Standardization, Ecosystem Governance, Regulatory Governance, Openness Culture, and Institutional Drivers.

7.3.2.1 Organizational and Institutional Dimensions

From an organizational and institutional perspective, important differences can be observed regarding the conditions that support analytics capability across the analyzed procurement OGD ecosystems. In terms of Data Interoperability, the Brazilian ecosystem presents substantially greater potential for cross-dataset linkage and integration due to the availability of complementary public datasets, including company registries, sanctions databases, invoices issued to the government, electoral information, and social programs. This broader ecosystem enables analytical applications involving entity resolution and relational analysis across multiple institutional domains. In contrast, the Dutch and European ecosystems present more limited interoperability conditions, particularly due to lower data granularity, reduced availability of complementary datasets, and stricter constraints on identifiable information disclosure.

These differences directly influence the Value-Adding potential of procurement OGD ecosystems. While the European ecosystem demonstrates stronger standardization and governance-oriented openness, the Brazilian ecosystem offers greater analytical flexibility

through broader possibilities for data integration, reuse, and exploratory analysis. In this context, the capacity to generate analytical value depends not only on intrinsic data quality dimensions, but also on the extent to which ecosystems support interoperability, relational linkage, and cross-domain analytical reuse.

Differences are also observed regarding Self-Governance and Ecosystem Governance. The European ecosystem demonstrates stronger institutional coordination, standardized reporting structures, and more centralized governance mechanisms, particularly through supranational initiatives such as TED. Similarly, the Dutch ecosystem reflects a more structured and coordinated administrative environment for procurement data publication. In contrast, the Brazilian ecosystem presents a more decentralized and heterogeneous governance arrangement involving multiple governmental entities and distinct publication practices. Although this decentralization introduces inconsistencies and coordination challenges, it also contributes to a broader and more diverse ecosystem of interconnected public datasets.

Regarding Policy Standardization, the European ecosystem demonstrates higher levels of harmonization through common metadata structures, standardized publication practices, and coordinated governance procedures across jurisdictions. The Brazilian ecosystem, while presenting lower formal standardization, provides greater flexibility for exploratory analytical applications due to the diversity and granularity of available data. These findings suggest that stronger standardization and coordination do not necessarily translate into greater analytics capability, particularly in analytical contexts that require detailed transactional and relational data.

Finally, Institutional Drivers also play a significant role in shaping procurement OGD ecosystems. In Brazil, pressure from oversight institutions, journalists, public prosecutors, and civil society has historically contributed to broader transparency practices and the publication of highly granular datasets. In the European and Dutch contexts, institutional drivers appear to be more strongly associated with governance harmonization, standardization, and regulatory compliance. Together, these differences reinforce that analytics capability emerges not only from technical data quality characteristics, but also from broader organizational and institutional conditions that influence interoperability, governance coordination, standardization, and analytical reuse across procurement OGD ecosystems.

7.3.2.2 Legal and Regulatory Dimensions

From a legal and regulatory perspective, important differences can be observed regarding how procurement OGD ecosystems balance transparency, data disclosure, governance, and privacy protection. In terms of Regulatory Governance, the European ecosystem is strongly influenced by formal regulatory frameworks and supranational governance mechanisms that prioritize standardization, legal conformity, and data protection principles. In particular, regulations such as the GDPR contribute to a more restrictive environment regarding the disclosure and reuse of identifiable and relational procurement information. These restrictions directly affect the interoperability and analytical reuse of procurement-related data, particularly in applications involving entity linkage, network analysis, anomaly detection, and fraud tracing.

Although the Brazilian LGPD was strongly inspired by the GDPR, the operational implications observed in the Brazilian ecosystem differ substantially from the European context. In practice, the Brazilian ecosystem demonstrates a more flexible interpretation of data disclosure practices, resulting in broader availability of granular procurement data and greater possibilities for analytical integration across datasets. As a result, while the European and Dutch ecosystems demonstrate stronger formal governance maturity in terms of regulatory compliance and standardized disclosure procedures, the Brazilian ecosystem offers greater practical openness for analytical and data-driven applications.

These findings reinforce that legal and regulatory conditions play a central role in shaping the analytics capability of procurement OGD ecosystems. More specifically, they suggest that regulatory governance influences not only how procurement data is disclosed, but also the extent to which ecosystems can support interoperability, analytical reuse, relational analysis, and advanced data-driven applications in public procurement.

7.3.2.3 Cultural Dimensions

Cultural conditions also play a significant role in shaping the characteristics and analytics capability of procurement OGD ecosystems. In terms of Collaboration Culture, the Brazilian ecosystem demonstrates broader practices related to transparency, public scrutiny, and cross-domain analytical reuse. The availability of multiple interconnected public datasets and the active participation of oversight institutions, journalists, researchers, and civil society contribute to a more collaborative environment for data sharing and analytical exploration. These conditions facilitate the development of applications involving entity

linkage, relational analysis, and fraud detection across different governmental domains.

In contrast, the European and Dutch ecosystems appear to adopt a more controlled and governance-oriented model of openness, emphasizing standardization, privacy protection, and formal disclosure procedures. While these characteristics contribute to stronger governance maturity and regulatory conformity, they also create a more constrained environment for exploratory analytical reuse and cross-domain integration. As a result, collaboration practices related to interoperability and data sharing tend to be more limited when compared to the Brazilian context.

Differences are also observed regarding Openness Culture. The Brazilian ecosystem reflects a stronger disclosure-oriented transparency culture, influenced by oversight practices, public accountability demands, and broader expectations regarding access to governmental information. Conversely, the European and Dutch ecosystems demonstrate a more balanced approach between openness and privacy protection, resulting in stricter controls over identifiable and relational information. Together, these findings suggest that cultural orientations toward collaboration, openness, and transparency directly influence the extent to which procurement OGD ecosystems can support interoperability, analytical reuse, and data-driven applications in public procurement.

7.4 Final Remarks

Figure 7.3 presents an integrated comparative assessment of the procurement OGD ecosystems analyzed in this study, combining both the quantitative data quality dimensions and the qualitative dimensions associated with analytics capability. The figure summarizes the extent to which each ecosystem demonstrates favorable technical and socio-technical conditions for supporting analytical usability, data-driven decision-making, and value generation through procurement-related OGD.



Figure 7.3: Integrated Comparative Assessment of Data Quality and Analytics Capability in Procurement OGD Ecosystems

Regarding the quantitative assessment, the classifications associated with the Data Quality dimensions were derived from the average values obtained for each dimension during the quantitative evaluation stage. The classifications follow four interpretative levels: Empty, Low, Medium, and High. More specifically, dimensions with average values equal to zero were classified as Empty, values between 0 and 0.5 as Low, values between 0.5 and 0.9 as Medium, and values equal to or above 0.9 as High. From this perspective, the figure highlights that Brazil and the European Union generally present stronger conditions regarding dimensions such as Currentness, Understandability, Accuracy, and Compliance, while differences become more evident in dimensions such as Traceability and Completeness. The Dutch ecosystem, in contrast, demonstrates comparatively lower conditions in some dimensions associated with data linkage and structural completeness.

In the qualitative assessment, the classifications associated with Analytics Capability dimensions were derived from a comparative interpretative analysis grounded in the socio-technical dimensions previously presented in Table 7.4. Rather than representing mathematically calculated scores, these classifications reflect the extent to which each ecosystem demonstrates favorable conditions for supporting analytics capability through aspects related to interoperability, governance arrangements, institutional coordination, openness practices, regulatory environments, collaboration culture, and value generation potential. In this context, classifications identified as High indicate stronger evidence of socio-technical conditions supporting analytics capability and analytical usability, Medium reflects intermediate or balanced conditions, while Low represents more limited conditions for enabling analytical integration and data-driven applications.

Taken together, the integrated assessment reinforces that intrinsic data quality dimensions alone are insufficient to explain the analytical potential of procurement OGD ecosystems. While technical quality remains an important foundational condition, the results suggest that analytics capability emerges from the interaction between technical and socio-technical dimensions. More specifically, the findings indicate that interoperability mechanisms, governance structures, institutional coordination, regulatory arrangements, and cultural orientations toward openness and collaboration play a central role in shaping the capacity of procurement OGD ecosystems to support technological solutions, analytical applications, and evidence-based policymaking in governmental contexts.

The results of this study suggest that higher levels of formal data quality do not necessarily translate into greater analytics capability. Although the UE dataset achieved better results in dimensions related to compliance, standardization, metadata structures,

and formal openness, the Brazilian ecosystem demonstrated greater analytical flexibility due to its higher data granularity, broader availability of complementary datasets, and stronger interoperability potential. These findings are aligned with the perspective proposed by (LNENICKA et al., 2024), which argues that the value generation potential of public data ecosystems depends not only on the quality and availability of datasets, but also on ecosystem characteristics that enable interoperability, integration, reuse, and cross-domain analytical exploration. In this sense, analytics capability can be understood as the capacity of an OGD ecosystem to effectively support analytical and data-driven applications, relational analysis, and decision-support processes. Consequently, the findings suggest the need for focusing on evaluating the analytics capability of OGD ecosystems beyond traditional metrics of data quality.

Similarly, the findings also suggest that transparency does not necessarily imply analytical transparency, since procurement data may be publicly available while still remaining analytically opaque due to limitations related to granularity, interoperability, cross-domain linkage, and machine-oriented reuse. In this sense, transparency-oriented disclosure differs from analytically actionable transparency, particularly in OGD ecosystems primarily designed to satisfy compliance, governance, accountability, or formal disclosure obligations rather than to support analytical exploration, AI applications, and decision-support systems. These results are aligned with the perspectives proposed by (ALTAYAR, 2018) and (KASSEN, 2018), which emphasize that organizational motivations, governance structures, institutional arrangements, and transparency cultures directly influence how OGD ecosystems are designed and coordinated. As a result, datasets may achieve high levels of formal transparency while still presenting limited capability to support analytical reuse and intelligence generation.

In this sense, ecosystem architecture matters because socio-technical conditions matter, and socio-technical conditions themselves are deeply influenced by institutional, organizational, legal and cultural contexts. Consequently, OGD maturity models should evolve toward approaches capable of incorporating analytics capability and analytical usability dimensions, recognizing that governments must define not only whether procurement data should be publicly available, but also for what purpose such data is being disclosed, rather than solely satisfying auditing or compliance requirements. In this study, Table 7.4 summarized the main socio-technical conditions identified as relevant for analytics capability and value-adding within procurement OGD ecosystems. These findings also reinforce the importance of future comparative studies involving different countries, governance arrangements, and procurement portals to better understand how cultural, organizational,

territorial, and institutional factors shape the analytics capability of procurement-related OGD ecosystems across distinct contexts.

Chapter 8

Discussions

This chapter moves beyond the technical specification and validation of the proposed reference model to situate its contributions within a broader reflection on data driven solutions, institutional transformation, and science based decision making in the public sector. Rather than merely summarizing empirical findings, the discussion critically examines how the model reconfigures fraud risk analysis as a structured socio technical system grounded in data infrastructures, analytical intelligence, and accountable human judgment. By exploring the role of open and institutional data as foundational assets, the organizational implications for oversight bodies, the construction of public policy based on empirical evidence, the appropriate positioning of AI within democratic systems, and the relevance of DSR as a methodological foundation for public innovation, this chapter articulates the wider societal, governmental, and theoretical implications of the thesis. In doing so, it frames the reference model not only as a technical artifact, but as a contribution to the evolution of scientifically informed and ethically grounded digital government.

8.1 Data as the infrastructure of scientific government

The increasing digitization of public administration has transformed data from a by product of bureaucratic processes into a foundational infrastructure for value generation. In contemporary digital states, data are no longer merely records of past actions, but structured representations of reality, enabling observation, measurement, and inference about governmental activity. Just as scientific progress depends on systematic data collection and analytical rigor, scientifically informed government depends on reliable, accessible, and governable data infrastructures. In this sense, data constitute the epistemic foundation upon which evidence-based decision making, risk assessment, and institutional

accountability are constructed.

8.1.1 Data as epistemic infrastructure and institutional awareness

In contemporary digital government, data function as the epistemic infrastructure upon which institutional awareness and decision-making capacity are constructed. Whether openly published or institutionally restricted, datasets acquire strategic value not by virtue of their accessibility alone, but by capable of transforming information into structured knowledge. Governmental action must be grounded in evidence-based reasoning supported by reliable, traceable, and analytically coherent data systems.

Governments simultaneously operate as producers and consumers of knowledge. Through administrative processes, regulatory activities, procurement transactions, and service delivery, public institutions continuously generate large volumes of structured data. Yet the mere existence of data does not guarantee institutional intelligence. Data must be systematically collected, harmonized, modeled, and interpreted to produce actionable insight. In this sense, government can be understood as a knowledge producing system, where the continuous generation and analysis of experimental data enable the advancement of theoretical understanding. Similarly, a scientifically oriented state derives institutional knowledge from the systematic processing of administrative data.

This transformation from data availability to institutional awareness follows a logic aligned with the scientific method: observation of empirical phenomena, modeling of relationships and patterns, inference based on analytical procedures, and decision making grounded in structured evidence. When applied to public administration, this cycle redefines governance as a process of empirically informed reasoning rather than discretionary intuition. Figure 8.1 illustrates this epistemic cycle, highlighting how administrative phenomena are captured through data infrastructures, enabling analytical modeling and inference processes that ultimately support decision-making. The cycle is further grounded in policy and implementation contexts, ensuring that insights generated from data are translated into concrete governmental actions. This perspective reinforces the role of data as a foundational element for institutional learning and continuous improvement in public sector decision-making.

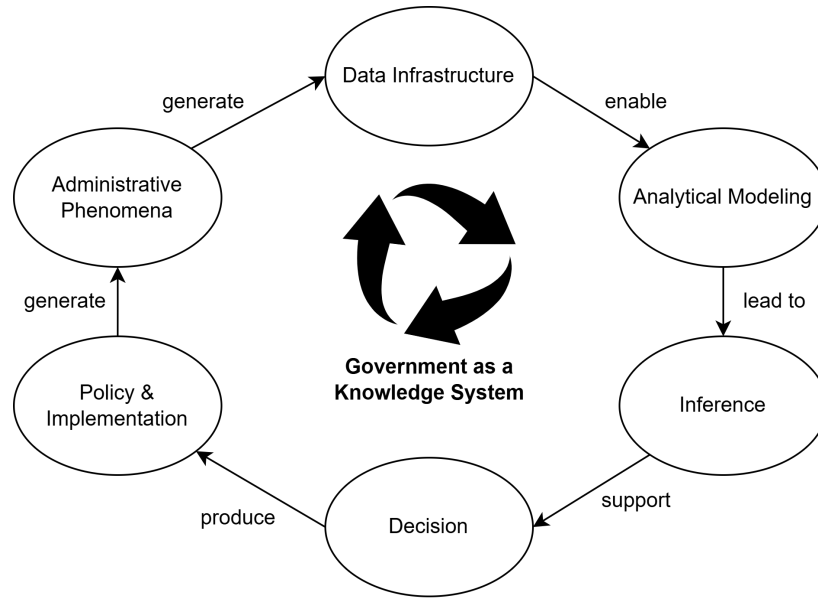


Figure 8.1: Epistemic Cycle of Scientific Government. Inspired by (HOUGHTON, 2009)

8.1.2 Data provenance as a governance mechanism

If data constitute the epistemic infrastructure of scientific government, provenance constitutes its structural mechanism of accountability. Provenance does not merely record the technical lineage of data transformations, it operationalizes traceability as an institutional principle. By documenting how data are generated, transformed, interpreted, and used in decision-making processes, provenance establishes a structured chain of responsibility that connects analytical outputs to their underlying sources, methods, and actors.

In this sense, provenance performs four interrelated governance functions. First, it enables responsibility by explicitly linking decisions and analytical results to identifiable agents and procedures. Second, it strengthens transparency by making visible the intermediate steps between raw administrative data and institutional conclusions. Third, it enhances auditability by allowing independent verification of analytical processes and methodological assumptions. Finally, it ensures traceability, which becomes a democratic condition for the legitimate use of data-driven systems in public administration.

In democratic systems, public power must be explainable and contestable. When analytical models, particularly those incorporating ML techniques, inform oversight actions or policy decisions, the absence of traceable reasoning paths may undermine institutional legitimacy. Provenance addresses this risk by embedding structured documentation within the analytical lifecycle itself.

Within the reference model proposed in this thesis, provenance is therefore positioned

not as an auxiliary metadata layer, but as a foundational governance mechanism that sustains the integrity of the epistemic cycle. By ensuring that every risk indicator, inference, and decision can be reconstructed and examined, provenance transforms data-driven oversight from a purely technical exercise into a transparent, accountable, and democratically aligned institutional practice.

8.2 Organizational and institutional implications for oversight bodies

The transition toward data driven and provenance-aware oversight systems requires a profound cultural transformation within audit institutions. Traditionally, public auditing has operated predominantly under a reactive paradigm, triggered by complaints, external reports, or ex post verification of suspected irregularities. The incorporation of structured data infrastructures and predictive analytical models reorients this logic toward a proactive and risk based approach, in which potential anomalies can be identified before they materialize into confirmed misconduct. This shift demands not only the adoption of technological tools but also a reconfiguration of professional mindset and institutional capacity: auditors must increasingly engage with probabilistic reasoning, logic reasoning, risk prioritization, and model supported inference. Data literacy, statistical reasoning, and technological fluency become essential components of the auditor's professional profile. In this context, analytical outputs do not replace human judgment but reshape its scope, moving audit practice from retrospective validation toward anticipatory institutional intelligence.

The systematic use of red flags as structured risk indicators contributes to the standardization and professionalization of oversight activities. In environments characterized by heterogeneous datasets and decentralized procurement systems, the absence of shared analytical criteria often leads to fragmented and discretionary evaluations. By operationalizing red flags as formally defined, empirically grounded, and traceable indicators, oversight bodies establish a common technical language for risk assessment. This standardization enhances methodological coherence across cases, reduces interpretative arbitrariness, and facilitates inter-institutional coordination. Moreover, the explicit linkage between indicators, data sources, and analytical procedures strengthens professional accountability, transforming risk assessment from an implicit expertise based activity into a structured and reproducible institutional process.

8.3 Science based decision making and public policy construction

A government oriented toward scientific evidence operates under the premise that public decisions should be informed by structured observation, statistical reasoning, and analytically validated knowledge. Rather than relying predominantly on political intuition, ad hoc judgment, or episodic information, knowledge-driven governance institutionalizes the systematic use of data as a foundation for policy deliberation. In this model, administrative data, statistical analysis, and structured risk indicators become integral components of policy formulation and oversight prioritization. The objective is not to eliminate political discretion, but to anchor it within empirically grounded reasoning processes. By embedding analytical infrastructures into institutional routines, governments increase their capacity to detect systemic patterns, evaluate policy effectiveness, and allocate resources according to measurable risk and impact.

Empirical knowledge functions as a stabilizing pillar in policy design by constraining arbitrariness and enhancing rational justification. When policy formulation is supported by factual information, reproducible analytical procedures, and mathematically grounded evidence, decision making becomes more transparent and contestable. Statistical modeling and structured risk assessment introduce explicit criteria that can be examined, replicated, and debated. In the context of public procurement oversight, the transformation of heterogeneous administrative records into formalized red flags exemplifies how empirical reasoning can guide institutional action.

The integration of technical expertise into public policy construction raises a fundamental normative tension between competence and democratic representation. Policies cannot be reduced to purely technical exercises, nor can they rely solely on political negotiation detached from empirical reality. Scientific government therefore requires a balanced configuration in which technical knowledge informs decision making while remaining accountable to democratic oversight and public deliberation. The risk of technocracy emerges when analytical systems are treated as self-legitimizing authorities; conversely, the absence of technical competence may lead to uninformed or inefficient government. The challenge lies in designing institutional arrangements where expertise enhances democratic legitimacy rather than substituting it. In this configuration, data-driven models serve as decision-support instruments, while final authority remains anchored in accountable public institutions.

Figure 8.2 presents a conceptual representation of public policy construction as a structural equilibrium between three interdependent dimensions: empirical evidence, technical expertise, and democratic legitimacy. Empirical evidence provides the factual and statistical foundation for informed reasoning; technical expertise transforms data into structured interpretation and actionable models; and democratic legitimacy ensures that policy decisions remain accountable to public deliberation and institutional representation. Public policy design emerges at the intersection of these dimensions, reflecting a balanced configuration in which analytical rigor supports, but does not replace, democratic authority.

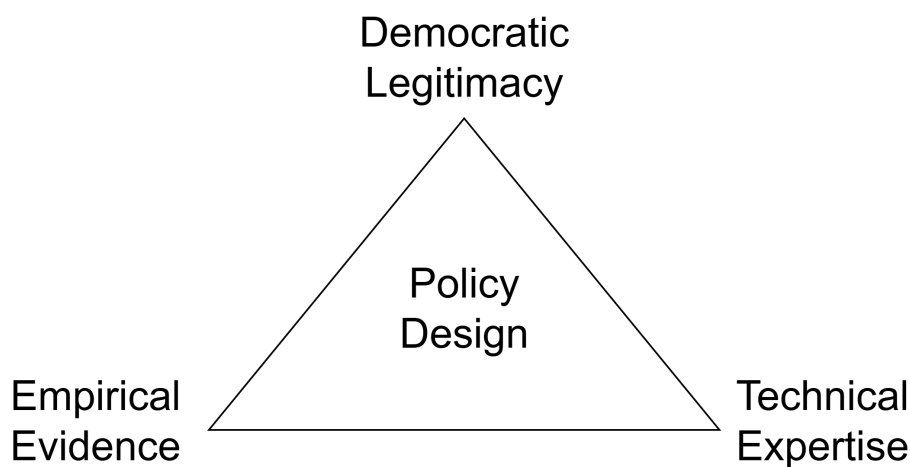


Figure 8.2: Structural balance between empirical evidence, technical expertise and democratic legitimacy in public policy design

8.4 AI as an instrument in digital government

AI has frequently been framed in public discourse as a transformative and self-sufficient solution capable of revolutionizing governmental processes. Such narratives, however, risk obscuring the structural and institutional conditions necessary for responsible implementation. AI does not autonomously generate governance improvements; it operates within pre-existing data infrastructures, organizational cultures, and regulatory environments. In the absence of reliable data governance, methodological rigor, and accountability mechanisms, algorithmic systems may amplify inefficiencies or introduce new forms of opacity. Deconstructing the AI hype therefore requires repositioning AI not as an autonomous actor of reform, but as a contingent analytical tool whose impact depends fundamentally on institutional design choices.

Within the framework proposed in this thesis, AI is conceptualized as decision support infrastructure rather than decision making authority. Analytical models serve to

structure information, identify patterns, and prioritize risks, but they do not possess normative competence or democratic legitimacy. The human in the loop configuration is therefore not an optional safeguard, but a structural requirement. Human oversight ensures contextual interpretation, ethical evaluation, and final accountability for institutional action. Responsibility remains exclusively anchored in public officials and institutions, even when algorithmic outputs inform their deliberations. By embedding AI within a provenance-aware and traceable decision-support architecture, oversight systems can leverage computational scalability while preserving institutional responsibility.

The integration of AI into oversight systems inevitably introduces structural trade-offs that must be consciously managed. Increased analytical efficiency may conflict with procedural accountability; higher levels of automation may reduce direct human engagement; scalability may challenge interpretability; and complex modeling techniques may compromise institutional transparency. These tensions are not merely technical constraints but normative design dilemmas. Responsible digital government requires explicit recognition of these trade-offs and deliberate institutional calibration between competing objectives. In the context of fraud risk analysis in public procurement, the adoption of AI must therefore be guided by governance oriented principles that balance performance gains with traceability, explainability, and democratic control. AI becomes sustainable within public administration only when embedded in structures that privilege accountability over mere optimization.

8.5 DSR as a methodological foundation for public sector innovation

DSR is frequently associated with the construction of technical artifacts; however, in public sector contexts, its scope necessarily extends beyond purely computational solutions. Public government problems are inherently sociotechnical, situated at the intersection of institutional norms, legal frameworks, organizational cultures, and technological infrastructures. The development of the proposed reference model illustrates how DSR functions as a bridge between theoretical constructs and the practical realities of audit institutions. Rather than producing isolated technical components, DSR enables the structured integration of conceptual rigor and contextual relevance. In this sense, the artifact designed in this thesis is not merely a system architecture, but a structured intervention in institutional reasoning practices.

Government innovation must be framed as a sociotechnical endeavor in which computational rigor and social responsibility are inseparably intertwined. Exact sciences contribute methodological precision, formal modeling, and analytical scalability; however, these capabilities acquire public value only when aligned with societal demands, normative expectations, and accountability structures. By integrating scientific methodologies with social imperatives, government innovation becomes a deliberate sociotechnical construction rather than a purely technological transformation.

The implications of this thesis extend beyond fraud risk analysis in PP, contributing to the consolidation of a structured research agenda for data driven digital government. In this context, DSR is not merely a methodological choice, but a foundational framework for government artifacts. Public sector innovation demands more than technological experimentation; it requires artifacts that are analytically robust, normatively defensible, and institutionally integrable. DSR provides the scaffolding for this construction by explicitly linking problem relevance, theoretical grounding, artifact design, and contextual evaluation within democratic settings. A research agenda for data-driven digital government must therefore prioritize not only performance metrics, but also institutional legitimacy as a core design criterion, positioning government artifacts as deliberate sociotechnical constructions rather than isolated technical solutions.

8.6 Final Remarks

This chapter has expanded the scope of the thesis beyond the technical aspects of the proposed reference model, positioning it within a broader transformation toward scientifically informed and institutionally accountable digital government. By framing data as epistemic infrastructure, provenance as a governance mechanism, and AI and analytics as decision support instrumentation, the discussion has emphasized that fraud risk analysis in PP cannot be reduced to computational efficiency. Rather, it must be understood as a structured sociotechnical system in which analytical rigor, organizational transformation, democratic legitimacy, and human accountability are mutually reinforcing components. The reference model thus emerges not merely as a technical solution, but as an institutional design proposition for embedding evidence based reasoning within public oversight.

More fundamentally, this chapter argues that data driven government is not achieved through technological adoption alone, but through deliberate institutional design grounded in methodological rigor. By employing DSR as a structuring framework, the thesis demon-

strates how governance-oriented artifacts can be systematically constructed to integrate analytical robustness with democratic accountability. In doing so, it contributes to a broader research agenda in digital government that prioritizes traceability, legitimacy, and epistemic responsibility as core design principles. The evolution toward scientific government is therefore not an automatic consequence of digitization, but the result of intentional sociotechnical engineering aimed at aligning data infrastructures, institutional practices, and public values.

Chapter 9

Conclusions

This thesis developed and instantiated a reference model for fraud risk analysis in PP grounded in the DSR paradigm. The research focused on constructing a structured artifact that integrates OGD, red flag and ML methods, provenance mechanisms, and ethical requirements into a coherent decision support arrangement. By following the cycles of DSR, the study systematically identified a practical problem, namely the fragmentation between analytical performance and institutional accountability, and translated it into design requirements operationalized within the proposed model. The resulting artifact offers a formalized blueprint that defines components, processes, actors, and governance mechanisms necessary for trustworthy supported fraud risk analysis in regulated public sector environments.

From a theoretical perspective, this thesis contributes to the Information Systems and Digital Government literature by conceptualizing fraud risk analysis in public procurement as a data-driven sociotechnical system formalized through a reference model. At its core, the model is structured around three interdependent analytical layers: the Data Layer, the Engine Layer, and the Decision Layer. Rather than centering the contribution on specific analytical techniques, the proposed model formalizes how structured government data (Data), computational intelligence mechanisms (Engine), and human-in-the-loop decision processes (Decision) operate as an integrated analytical framework. The Data Layer establishes the foundations for data acquisition, integration, harmonization, and quality assurance; the Engine Layer operationalizes intelligence through rule-based risk indicators and AI-supported analytical models; and the Decision Layer supports interpretation, prioritization, and human-centered audit decision-making. Complementing this analytical core, the reference model incorporates an Ethical Layer that embeds principles of transparency, accountability, explainability, and human oversight; a Provenance

Layer that ensures the traceability of data transformations and analytical outputs; a Governance and Security Layer that addresses institutional governance, access control, and operational security; and an Evaluation and Refinement Layer that supports continuous assessment, auditor feedback, and iterative improvement. The theoretical advancement lies in demonstrating that effective fraud risk analysis does not emerge from AI models alone, but from the coordinated interaction between analytical capabilities, governance mechanisms, and institutional processes. By integrating these complementary layers into a unified reference model, this thesis advances an architectural perspective in which analytical capability, trustworthiness, and institutional legitimacy are treated as mutually reinforcing design dimensions.

Practically, the proposed reference model contributes as a structured decision support tool for public auditors and oversight bodies engaged in fraud risk analysis in public procurement. Rather than positioning AI as an autonomous decision maker, the model operationalizes AI and advanced analytics techniques as institutional support mechanisms for auditing and inspection activities. By integrating data processes, red flag methods, predictive modeling, and traceability mechanisms within a coherent artifact, the reference model enables the systematic identification, prioritization, and justification of risk signals in procurement processes.

Academically, this research contributes to ongoing debates in Digital Government and IS by providing a concrete example of how DSR can be applied to ethically sensitive, data-intensive public sector problems. It demonstrates how technical innovation in data engineering, statistical modeling, and ML can be systematically aligned with institutional theory, audit practice, and ethical principles. By formalizing fraud risk analysis as a structured sociotechnical architecture, the thesis offers a replicable pathway for future research on decision support systems in government.

At a societal and policy level, the thesis highlights the potential of data-driven oversight tools to strengthen public integrity and social trust. By improving the transparency and effectiveness of fraud risk analysis in PP, such systems can contribute to better use of public resources, deterrence of corrupt practices, and increased confidence in public institutions.

9.1 Limitations

Despite the contributions presented in this thesis, several limitations must be acknowledged. These limitations are inherent to the research context, methodological choices, and scope of the proposed reference model, and they provide important context for interpreting the results and guiding future research.

First, the scope of artifact instantiation remains bounded. Although the reference model was validated with senior Brazilian public auditors and informed by comparative reflections between Brazil, European Union and the Netherlands, it was not implemented as a fully operational system across multiple governmental environments using production level data. The artifact remains at the level of a formalized reference model and partial instantiation, which limits empirical evidence regarding its performance under real world operational constraints.

Relatedly, the research does not include a longitudinal evaluation of impact. The study does not empirically measure long term outcomes such as measurable reductions in fraud incidence, improvements in audit efficiency, or behavioral changes among suppliers and contracting authorities. While the model was designed to enhance fraud risk analysis capabilities, its sustained institutional and economic effects remain to be empirically assessed over extended periods of deployment.

Another limitation concerns the dependency on the quality, structure, and availability of public procurement data. The proposed reference model assumes the existence of relatively structured, accessible, and interoperable open government datasets. In contexts characterized by low digital maturity, fragmented data infrastructures, or limited transparency policies, the applicability and effectiveness of the model may be significantly constrained. Data incompleteness, inconsistency, or lack of standardization may directly affect the performance of analytical components across the layers.

The generalization of the reference model to other national contexts must also be considered cautiously. Although the thesis incorporates comparative reflections between different institutional environments, regulatory, cultural, and administrative differences across countries may require substantial adaptation of governance mechanisms, risk indicators, and decision workflows. The model provides a structured blueprint, but its implementation may vary depending on legal frameworks, oversight traditions, and levels of institutional capacity.

Finally, the scope of the model is intentionally focused on PP. While its architectural

logic may be extensible to other domains of public oversight, the reference model was conceived and structured specifically for procurement processes. Application to other domains would require contextual adaptation of data models, risk indicators, and institutional mechanisms.

9.2 Future Works

The reference model proposed in this thesis opens several avenues for future research and practical development. These directions aim to extend the analytical scope, operational maturity, and institutional applicability of the artifact.

A primary direction involves the full empirical implementation of the proposed reference model within a governmental environment. Future studies should operationalize the model as an integrated system deployed in a public institution, enabling the evaluation of technical performance, usability by auditors, organizational integration, and real-world constraints. Such implementation would allow the transition from architectural validation to production-level experimentation, providing deeper insights into scalability, interoperability with legacy systems, and institutional adoption dynamics.

A second important research direction concerns longitudinal quantitative evaluation. Future work should assess the medium- and long-term impact of the model on audit efficiency, fraud detection rates, prioritization of high risk cases, and potential economic savings in public procurement.

Comparative cross national testing also represents a promising avenue for extension. Although the thesis incorporated comparative reflections between Brazil, European Union and the Netherlands, the model was not fully implemented in other context due to institutional and data access restrictions. Future research could apply the reference model in countries with varying levels of digital maturity, transparency frameworks, and regulatory environments to assess its adaptability and contextual robustness.

Another important extension involves adapting to other domains of public sector control. While this thesis focused specifically on public procurement, the architectural logic of integrating data infrastructures, analytical engines, and decision-support mechanisms may be transferable to areas such as public subsidies, infrastructure contracts, healthcare expenditure monitoring, among others. Future research could explore domain specific adaptations of the reference model, thereby broadening the applicability of the model across public administration contexts.

Finally, future studies may investigate the integration of sensitive or restricted-access datasets to complement open government data. While this research primarily relied on publicly available procurement information, incorporating tax records, beneficial ownership registries, financial intelligence data, or internal audit logs could significantly enhance risk modeling capabilities. Such extensions, however, would require careful attention to data protection regulations, ethical safeguards, and institutional governance mechanisms.

9.3 Final Remarks

In conclusion, this thesis demonstrates that fraud in public procurement can be addressed more effectively when data science, ethical AI, and audit practice are treated as interdependent components of a unified analytical framework. By combining interpretable red flags, data provenance, and explainable risk modeling within a decision support system designed for auditors, the research offers a concrete response to the challenges of transparency, scalability, and accountability in public-sector oversight.

More broadly, the work highlights the importance of interdisciplinary approaches in Digital Government research, showing that technological innovation alone is insufficient to address complex governance problems. Instead, meaningful progress emerges when computational methods are aligned with institutional realities, ethical principles, and professional practice. It is within this convergence of science, ethics, and public accountability that the proposed framework seeks to contribute—offering both a practical artifact and a conceptual foundation for future efforts to strengthen integrity and trust in public procurement.

References

- ABIORO, Tunde A. Public procurement corruption and service delivery in Nigeria and South Africa. In: PUBLIC procurement, corruption and the crisis of governance in Africa. [S.l.]: Springer, 2021. P. 249–267.
- ACHUA, Joseph K. Anti-corruption in public procurement in Nigeria: Challenges and competency strategies. **Journal of public procurement**, Emerald Publishing Limited, v. 11, n. 3, p. 323–333, 2011.
- ADENIRAN, Adewale Abayomi; ONEBUNNE, Amaka Peace; WILLIAM, Paul. Explainable AI (XAI) in healthcare: Enhancing trust and transparency in critical decision-making. **World Journal of Advanced Research and Reviews**, v. 23, n. 3, p. 2647–2658, 2024.
- ADEPOJU, ADEWUMI SUNDAY; CHINONYEREM, CONFIDENCE ADIMCHI. Advancing good governance through AI-powered oversight in the United States: Risks and opportunities for public institutions. **International Journal of Humanities, Literature and Art Research**, 2025.
- ADEWUSI, Bolanle A et al. A conceptual model for responsible AI integration in public-facing digital services and platform governance. **Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.**, v. 10, n. 3, p. 735–767, 2024.
- AI, HLEG. High-level expert group on artificial intelligence. **Ethics guidelines for trustworthy AI**, European Commission. Available at: <https://ec.europa.eu/digital-single...>, v. 6, 2019.
- ALDANA, Andrés; FALCÓN-CORTÉS, Andrea; LARRALDE, Hernán. A machine learning model to identify corruption in Mexico's public procurement contracts. **arXiv preprint arXiv:2211.01478**, 2022.
- ALFIAN, Adhi; RITCHI, Hamzah; ADRIANTO, Zaldy. Fraud analytics practices in public-sector transactions: a systematic review. **Journal of Public Budgeting, Accounting & Financial Management**, Emerald Publishing Limited, v. 35, n. 5, p. 685–710, 2023.

- ALMEIDA, Alvaro Santos; CIMA, Joana Ferreira. Demand uncertainty and hospital costs: an application to Portuguese public hospitals. **The European Journal of Health Economics**, Springer, v. 16, n. 1, p. 35–45, 2015.
- ALTAYAR, Mohammed Saleh. Motivations for open data adoption: An institutional theory perspective. **Government Information Quarterly**, Elsevier, v. 35, n. 4, p. 633–643, 2018.
- ALTURKI, Ahmad et al. Multi-dimensional fraud detection metrics in business processes and their application. **International Journal of Advanced Computer Science and Applications**, Science and Information (SAI) Organization Limited, v. 11, n. 9, 2020.
- ALVES BATISTA, Danielle. Enhancing transparency and accountability in public procurement: exploring blockchain technology to mitigate records fraud. **Records Management Journal**, Emerald Publishing Limited, v. 34, n. 2/3, p. 151–170, 2024.
- ALWASSITI, Ghadeer; MORTEZA, Shahbazi Nia. The Role of Artificial Intelligence in Optimising the Use of Islamic Shari’ah in Achieving Transparency to Combat Corruption in Government Contracts in Iraq. **Manchester Journal of Transnational Islamic Law & Practice**, v. 21, n. 2, 2025.
- AMIRUDDIN, Amiruddin et al. The Use of Artificial Intelligence (AI) in Internal Supervision to Reduce Fraud in the Public Procurement System in Indonesia. **ProBisnis: Jurnal Manajemen**, v. 15, n. 5, p. 769–780, 2024.
- AMORETTI, Francesco. International organizations ICTs policies: e-democracy and e-government for political development. **Review of policy research**, Wiley Online Library, v. 24, n. 4, p. 331–344, 2007.
- ANDERSON, Robert D; JONES, Alison; KOVACIC, William E. **Combating corruption and collusion in public procurement: A Challenge for Governments Worldwide**. [S.l.]: Oxford University Press, 2024.
- ANDERSSON, Per Erik; ARBIN, Katarina; ROSENQVIST, Christopher. Assessing the value of artificial intelligence (AI) in governmental public procurement. **Journal of Public Procurement**, Emerald Publishing Limited, 2025.
- ANSHARI, Muhammad; LIM, Syamimi Ariff. E-government with big data enabled through smartphone for public services: Possibilities and challenges. **International Journal of Public Administration**, Taylor & Francis, v. 40, n. 13, p. 1143–1158, 2017.

- APPELBAUM, Deniz. Securing big data provenance for auditors: The big data provenance black box as reliable evidence. **Journal of emerging technologies in accounting**, American Accounting Association, v. 13, n. 1, p. 17–36, 2016.
- ARAGANI, Venu Madhav; ANUMOLU, Venkateswara Rao; SELVAKUMAR, P. Democratization in the Age of Algorithms: Navigating Opportunities and Challenges. **Democracy and Democratization in the Age of AI**, IGI Global Scientific Publishing, p. 39–56, 2025.
- AVDASHEVA, SB; KORNEEVA, DV; YUSUPOVA, GF. Artificial intelligence against collusion: What (not) to expect? **Voprosy Ekonomiki**, NP Voprosy Ekonomiki, n. 4, 2025.
- BAJRACHARYA, Kritika. Big Data and Artificial Intelligence Integration in Modernizing Governance and Public Administration Practices. **Global Research Perspectives on Cybersecurity Governance, Policy, and Management**, v. 8, n. 12, p. 34–47, 2024.
- BAROT, Ruchika V. **Detecting Collusion in Public Procurement: A Comparative Study of Machine Learning Models**. 2024. PhD thesis – Concordia University.
- BECKER, Jörg; DELFMANN, Patrick; KNACKSTEDT, Ralf. Adaptive reference modeling: Integrating configurative and generic adaptation techniques for information models. In: REFERENCE modeling: Efficient information systems design through reuse of information models. [S.l.]: Springer, 2007. P. 27–58.
- BENMOHAMED, Nuria; SHEN, Jun; VLAHU-GJORGIEVSKA, Elena. Public value creation through the use of open government data in Australian public sector: A quantitative study from employees' perspective. **Government Information Quarterly**, Elsevier, v. 41, n. 2, p. 101930, 2024.
- BERMÚDEZ, Jorge Manuel Macías; FARIAS, Gisell Karina Arreaga; TORRES, Leonso Torres. **Procedure for the acquisition of goods and services in public procurement**. [S.l.]: Infinite Study, 2020. v. 37.
- BHAROSA, Nitesh. **Netcentric Information Orchestration. Assuring Information and System Quality in Public Safety Networks**. 2011. PhD thesis – TU Delft.

- BOUCHETARA, Mehdi; ZEROUTI, Messaoud; ZOUAMBI, Anais Radja. Leveraging artificial intelligence (AI) in public sector financial risk management: Innovations, challenges, and future directions. **EDPACS**, Taylor & Francis, v. 69, n. 9, p. 124–144, 2024.
- BRANDÃO, Michele A et al. Plus: A semi-automated pipeline for fraud detection in public bids. **Digital Government: Research and Practice**, ACM New York, NY, v. 5, n. 1, p. 1–16, 2024.
- BRASIL. **Estratégia Brasileira de Inteligência Artificial – EBIA**. [S.l.: s.n.], 2023. <https://www.gov.br/mcti/pt-br/acompanhe-omcti/transformacaodigital/inteligencia-artificial>. Ministério da Ciência, Tecnologia e Inovação. Acesso em: 10 abr. 2025.
- CAMPAS, Alexandra; IACOB, Nadina; SIMONELLI, Felice. How can interoperability stimulate the use of digital public services? An analysis of national interoperability frameworks and e-Government in the European Union. **Data & Policy**, Cambridge University Press, v. 4, e19, 2022.
- CASTRO RODRIGUES, Diego de; LIMA, Márcio Dias de; BARBOSA, Rommel M. Fraud detection in social income transfer programs: A social data mining approach applied to data from Brazil. **SN Social Sciences**, Springer, v. 2, n. 9, p. 170, 2022.
- CATH, Corinne. Governing artificial intelligence: ethical, legal and technical opportunities and challenges. **Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences**, The Royal Society Publishing, v. 376, n. 2133, p. 20180080, 2018.
- CHARALABIDIS, Yannis et al. The world of open data. **Public Administration and Information Technology**. Cham: Springer International Publishing. doi, Springer, p. 978–3, 2018.
- CHAWLA, Siddharth Rachit. Ethical AI Starts with Data Provenance: A FATE Perspective. **International Journal of Computer Technology and Electronics Communication**, v. 4, n. 2, p. 3405–3409, 2021.
- CHORNYI, Kyrylo; SHILO, Galina; LEBEDIEVA-DYCHKO, Anastasiia. Analysis of state register data to identify anomalies and corruption threats in tenders and procurements. **The Second International Conference of Young Scientists on Artificial Intelligence for Sustainable Development (YAISD)**, 2025.

- CONCHA, Gaston et al. E-Government procurement observatory, maturity model and early measurements. **Government Information Quarterly**, Elsevier, v. 29, s43–s50, 2012.
- CRUZ, Eduardo et al. Detecting anomalous suppliers in electronic procurement systems using GAAN. In: IEEE. 2023 IEEE International Conference on Big Data (BigData). [S.l.: s.n.], 2023. P. 4147–4155.
- DAVIS, Daniel Bruno; MENDOZA, Ronald U; YAP, Jurel K. Corruption risk and political dynasties: exploring the links using public procurement data in the Philippines. **Economics of Governance**, Springer, v. 25, n. 1, p. 81–109, 2024.
- DECAROLIS, Francesco; GIORGIANTONIO, Cristina. Corruption red flags in public procurement: new evidence from Italian calls for tenders. **EPJ Data Science**, Springer Berlin Heidelberg, v. 11, n. 1, p. 16, 2022.
- DELLO, Amani; YOSHIDA, Chika. Online tendering and evaluation for public procurement in Tanzania. In: IEEE. 2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). [S.l.: s.n.], 2017. P. 137–141.
- DEMETER, Gabriel et al. Assessing the Impact of Supplier Group Stability on Public Procurement Performance in Slovakia: A Causal Forest Analysis of Collusion Signals. **IEEE Access**, IEEE, 2025.
- DESAI, Angel N et al. Real-time epidemic forecasting: challenges and opportunities. **Health security**, Mary Ann Liebert, Inc., publishers 140 Huguenot Street, 3rd Floor New . . . , v. 17, n. 4, p. 268–275, 2019.
- DOMASHOVA, Jenny; KRIPAK, Elena. Application of machine learning methods for risk analysis of unfavorable outcome of government procurement procedure in building and grounds maintenance domain. **Procedia Computer Science**, Elsevier, v. 190, p. 171–177, 2021.
- DOMINGOS, Silvio L et al. Identifying it purchases anomalies in the Brazilian Government Procurement System using deep learning. In: IEEE. 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA). [S.l.: s.n.], 2016. P. 722–727.
- DOUTHIT, Brian J et al. A conceptual framework of data readiness: the contextual intersection of quality, availability, interoperability, and provenance. **Applied Clinical Informatics**, Georg Thieme Verlag KG, v. 12, n. 03, p. 675–685, 2021.

- DUGUAY, Raphael; RAUTER, Thomas; SAMUELS, Delphine. The impact of open data on public procurement. **Journal of Accounting Research**, Wiley Online Library, v. 61, n. 4, p. 1159–1224, 2023.
- ENGİN, Zeynep; TRELEAVEN, Philip. Algorithmic government: Automating public services and supporting civil servants in using data science technologies. **The Computer Journal**, OUP, v. 62, n. 3, p. 448–460, 2019.
- FANG, Zhiyuan. E-government in digital era: concept, practice, and development. **International journal of the Computer, the Internet and management**, v. 10, n. 2, p. 1–22, 2002.
- FAZEKAS, Mihály; ABDOL, Aly, et al. Development aid contracts database: World Bank, Inter-American Development Bank, and EuropeAid. **Data in Brief**, Elsevier, v. 42, p. 108121, 2022.
- FAZEKAS, Mihály; BLUM, Jürgen René. Improving public procurement outcomes. **Policy research working paper**, v. 2, n. 4, p. 2–3, 2021.
- FAZEKAS, Mihály; KOCSIS, Gábor. Uncovering high-level corruption: cross-national objective corruption risk indicators using public procurement data. **British Journal of Political Science**, Cambridge University Press, v. 50, n. 1, p. 155–164, 2020.
- FAZEKAS, Mihály; TÓTH, Bence; ABDOL, Aly, et al. Global contract-level public procurement dataset. **Data in Brief**, Elsevier, v. 54, p. 110412, 2024.
- FAZEKAS, Mihály; TÓTH, István János; KING, Lawrence Peter. An objective corruption risk index using public procurement data. **European Journal on Criminal Policy and Research**, Springer, v. 22, n. 3, p. 369–397, 2016.
- FAZEKAS, Mihály; WACHS, Johannes. Corruption and the network structure of public contracting markets across government change. **Politics and Governance**, v. 8, n. 2, p. 153–166, 2020.
- FELIZZOLA, Heriberto et al. Enhancing transparency in public procurement: A data-driven analytics approach. **Information Systems**, Elsevier, v. 125, p. 102430, 2024.
- FERWERDA, Joras; DELEANU, Ioana; UNGER, Brigitte. Corruption in public procurement: finding the right indicators. **European journal on criminal policy and research**, Springer, v. 23, n. 2, p. 245–267, 2017.

- FINK, Katherine. Opening the government's black boxes: freedom of information and algorithmic accountability. **Information, Communication & Society**, Taylor & Francis, v. 21, n. 10, p. 1453–1471, 2018.
- FLOURIS, Giorgos et al. Using provenance for quality assessment and repair in linked open data. **11th International Semantic Web Conference**, Informatica, 2012.
- FREMPONG, David et al. Real-time analytics dashboards for decision-making using Tableau in public sector and business intelligence applications. **Journal of Frontiers in Multidisciplinary Research**, Anfo Publication House, v. 3, n. 2, p. 65–80, 2022.
- FUERTES, Mateo et al. Predicting Early Corruption Risk in Public Procurement: Ecuador's Case Study. In: IEEE. 2025 IEEE Ninth Ecuador Technical Chapters Meeting (ETCM). [S.l.: s.n.], 2025. P. 1–6.
- GADE, Kishore Reddy. Data-driven decision making in a complex world. **Journal of computational innovation**, v. 1, n. 1, 2021.
- GALLEGO, Jorge; RIVERO, Gonzalo; MARTÍNEZ, Juan. Preventing rather than punishing: An early warning model of malfeasance in public procurement. **International Journal of Forecasting**, Elsevier, v. 37, n. 1, p. 360–377, 2021.
- GAVUROVA, Beata; TUČEK, David; KOVÁČ, Viliam. Economic aspects of public procurement parameters in tertiary education sector. **Administratie si Management Public**, Bucharest University of Economic Studies Publishing House, 2019.
- GIBREEL, Omer; HONG, Ahreum. A holistic analysis approach to social, technical, and socio-technical aspect of e-government development. **Sustainability**, MDPI, v. 9, n. 12, p. 2181, 2017.
- GNALDI, Michela; DEL SARTO, Simone. Measuring corruption risk in public procurement over emergency periods. **Social Indicators Research**, Springer, v. 172, n. 3, p. 859–877, 2024.
- GOMES, Wesckley Faria; COLAÇO, Methanias. Applications of Artificial Intelligence for Auditing and Classification of Incongruent Descriptions in Public Procurement. In: XVIII Brazilian Symposium on Information Systems. [S.l.: s.n.], 2022. P. 1–8.
- GRAYCAR, Adam. Mapping corruption in procurement. **Journal of Financial Crime**, Emerald Publishing Limited, v. 26, n. 1, p. 162–178, 2019.
- HEGGSTAD, Kari K; FRØYSTAD, Mona. The basics of integrity in procurement. **U4 Issue**, v. 2011, n. 10, 2011.

- HERMAN, Surijadi; YOHANNIS, Tamaela Eduard. The effect of accountability, transparency, openness, fairness and competition on effectiveness and efficiency of e-procurement in Maluku Provincial procurement services unit. **Russian Journal of Agricultural and Socio-Economic Sciences**, Russian Journal of Agricultural and Socio-Economic Sciences, v. 79, n. 7, p. 113–122, 2018.
- HEVNER, Alan R. A three cycle view of design science research. **Scandinavian journal of information systems**, v. 19, n. 2, p. 4, 2007.
- HEVNER, Alan R et al. Design science in information systems research. **MIS quarterly**, JSTOR, p. 75–105, 2004.
- HICKOK, Merve. Public procurement of artificial intelligence systems: new risks and future proofing. **AI & society**, Springer, v. 39, n. 3, p. 1213–1227, 2024.
- HORNE, Juanida; VENTER, Jan; LOCHNER, Hennie. The red flag system as the gatekeeper in tender fraud prevention and detection of misrepresentation. **International Journal of African Renaissance Studies-Multi-, Inter-and Transdisciplinarity**, Taylor & Francis, v. 13, n. 1, p. 129–143, 2018.
- HOUGHTON, Luke. Generalization and systemic epistemology: Why should it make sense? **Systems Research and Behavioral Science: The Official Journal of the International Federation for Systems Research**, Wiley Online Library, v. 26, n. 1, p. 99–108, 2009.
- AL-INIZI, Mahdi Salah Mahdi. Enhancing Governmental Decision-Making through Predictive Analytics with Machine Learning-Based Data-Driven Framework. **Babylonian Journal of Machine Learning**, v. 2025, p. 86–96, 2025.
- INTERNATIONAL, Dama. **DAMA-DMBOK: Data management body of knowledge**. [S.l.]: Technics Publications, LLC, 2017.
- KALE, Amruta et al. Provenance documentation to enable explainable and trustworthy AI: A literature review. **Data Intelligence**, MIT Press One Rogers Street, Cambridge, MA 02142-1209, USA journals-info ..., v. 5, n. 1, p. 139–162, 2023.
- KAN, Celal Hakan et al. Artificial intelligence (ai) in the age of democracy and human rights: normative challenges and regulatory perspectives. **International Journal of Eurasian Education and Culture**, v. 9, n. 25, p. 145–166, 2024.
- KASSEN, Maxat. Open data and its institutional ecosystems: A comparative cross-jurisdictional analysis of open data platforms. **Canadian Public Administration**, Wiley Online Library, v. 61, n. 1, p. 109–129, 2018.

- KAZBEKOVA, Aissulu et al. Risk modelling as a way to diagnose corruption in procurement system: Practice and legislation. **Social and Legal Studies**, p. 299–309, Mar. 2025. DOI: 10.32518/sals1.2025.299.
- KETTEMANN, Dr Matthias C. UNESCO Recommendation on the Ethics of Artificial Intelligence. **Conditions for the Implementation in Germany**, 2022.
- KITCHENHAM, Barbara. Procedures for performing systematic reviews. **Keele, UK, Keele University**, Citeseer, v. 33, n. 2004, p. 1–26, 2004.
- KOWALKIEWICZ, Marek; DOOTSON, Paula. Government 5.0: the future of public services. **Chair in Digital Economy**, The Chair in Digital Economy, 2019.
- KULLMANN, Miriam. Promoting social and environmental sustainability: what role for public procurement. **Comp. Lab. L. & Pol’y J.**, HeinOnline, v. 40, p. 109, 2018.
- KUMAR, Anjali; NAIR, Arvind; PIECHA, Juliane. Measuring efficiency in international public procurement. **Journal of public procurement**, Emerald Publishing Limited, v. 15, n. 3, p. 365–389, 2015.
- KYRIAKOU, Kyriakos; OTTERBACHER, Jahna. In humans, we trust: Multidisciplinary perspectives on the requirements for human oversight in algorithmic processes. **Discover Artificial Intelligence**, Springer, v. 3, n. 1, p. 44, 2023.
- LABORATÓRIO DE INOVAÇÃO EM GOVERNO, GNova et al. Portal Nacional de Contratações Públicas. **Escola Nacional de Administração Pública (Enap)**, Escola Nacional de Administração Pública (Enap), 2021.
- LIMA, Wesley et al. Methodology for automatic extraction of red flags in public procurement. In: IEEE. 2023 International Joint Conference on Neural Networks (IJCNN). [S.l.: s.n.], 2023. P. 01–07.
- LINDGREN, Ida. Exploring the use of robotic process automation in local government. In: CEUR-WS. EGOV-CEDEM-EPART 2020 Virtual, Linköping 31 August 2020 through 2 September 2020. [S.l.: s.n.], 2020. v. 2797, p. 249–258.
- LISCIANDRA, Maurizio; MILANI, Riccardo; MILLEMACI, Emanuele. A corruption risk indicator for public procurement. **European Journal of Political Economy**, Elsevier, v. 73, p. 102141, 2022.
- LNENICKA, Martin et al. Understanding the development of public data ecosystems: from a conceptual model to a six-generation model of the evolution of public data ecosystems. **Telematics and informatics**, Elsevier, v. 94, p. 102190, 2024.

- LU, Jie et al. Data-driven decision-making (d 3 m): Framework, methodology, and directions. **IEEE transactions on emerging topics in computational intelligence**, IEEE, v. 3, n. 4, p. 286–296, 2019.
- LUNA-REYES, Luis F; GIL-GARCIA, J Ramon. Digital government transformation and internet portals: The co-evolution of technology, organizations, and institutions. **Government information quarterly**, Elsevier, v. 31, n. 4, p. 545–555, 2014.
- LUNDBERG, Scott M; LEE, Su-In. A unified approach to interpreting model predictions. **Advances in neural information processing systems**, v. 30, 2017.
- LUNGU, Maria. Enhancing public service delivery in government procurement: A review exploring the role of artificial intelligence and automative structures. **Handbook of Public Service Delivery**, Edward Elgar Publishing, p. 188–204, 2024.
- LYRA, Marcos S et al. Fraud, corruption, and collusion in public procurement activities, a systematic literature review on data-driven methods. **Applied Network Science**, Springer, v. 7, n. 1, p. 83, 2022.
- MAGAKWE, Jack. Advancing governance: Role of data analytics in driving evidence-based decision-making in public administration. In: RECENT advances in public sector management. [S.l.]: IntechOpen, 2025.
- MANTA, Otilia; MANSI, Eglá. The impact of globalization on innovative public procurement: Challenges and opportunities. **Administrative sciences**, MDPI, v. 14, n. 4, p. 80, 2024.
- MANTZARIS, EA. **Public procurement, tendering and corruption: Realities, challenges and tangible solutions**. 2014. PhD thesis – University of Pretoria.
- MARCH, Salvatore T; SMITH, Gerald F. Design and natural science research on information technology. **Decision support systems**, Elsevier, v. 15, n. 4, p. 251–266, 1995.
- MARCHESSAULT, Lindsey; KLUTTZ, Carey; FERNÁNDEZ, Mariana López. Bids, bias, and barriers: Approaches and challenges in using data to measure corruption and gender participation in public procurement. **Routledge Handbook of Gender and Corruption**, Routledge, p. 242–266, 2025.
- MARTÍNEZ-PLUMED, Fernando et al. SALER: a data science solution to detect and prevent corruption in public administration. In: SPRINGER. JOINT European Conference on Machine Learning and Knowledge Discovery in Databases. [S.l.: s.n.], 2018. P. 103–117.

- MATTHEW, Kalubanga; PATRICK, Kakwezi; DENISE, Kayiise. The effects of fraudulent procurement practices on public procurement performance. **International Journal of Business and Behavioural Sciences**, v. 3, n. 1, p. 17–27, 2013.
- MAVIDIS, Aristotelis; FOLINAS, Dimitrios; SKIADAS, Dimitrios. Unveiling the Research Landscape of Public Procurement and Emerging Technologies: A Topic Modelling Approach to Bibliometric Analysis and Co-occurrence Network Study: Exploring Innovations and Strategies in Government Acquisitions and Technological Advancements. **Digital Government: Research and Practice**, ACM New York, NY, v. 6, n. 4, p. 1–26, 2025.
- MCCUE, Clifford P; PITZER, Jack T. Centralized vs. decentralized purchasing: Current trends in governmental procurement practices. **Journal of Public Budgeting, Accounting & Financial Management**, Emerald Publishing Limited, v. 12, n. 3, p. 400–420, 2000.
- MENKE, Wagner; GOMES, Ricardo; XAVIER, Flávia. Impacts of AI-based anti-corruption audits on risk aversion in decision-making: a case study of the Brazilian ALICE tool. **Global Public Policy and Governance**, Springer, v. 4, n. 3, p. 273–286, 2024.
- MICHAEL, Achu Ann. Prevention and Detection of Bid Rigging in Public Procurement in India: Role of Artificial Intelligence. **World Competition**, v. 47, n. 3, 2024.
- MILANI, Riccardo. **Multi-level Corruption Risk Indicators in the Italian Public Procurement**. 2019. PhD Thesis – International Ph.D. in Criminology - Università Cattolica del Sacro Cuore, Milan, Italy.
- MODRUŠAN, Nikola; RABUZIN, Kornelije; MRŠIC, Leo. Review of public procurement fraud detection techniques powered by emerging technologies. **International Journal of Advanced Computer Science and Applications**, Science and Information (SAI) Organization Limited, v. 12, n. 2, p. 1–9, 2021.
- MOHD, Saifuddin; IJAB, Mohamad Taha. Leveraging Business Intelligence and Text Mining for Automated Detection of Public Procurement Fraud. In: SPRINGER. INTERNATIONAL Visual Informatics Conference. [S.l.: s.n.], 2025. P. 346–358.
- MOHD, Saifuddin; NOHUDDIN, Puteri NE. A Framework of Procurement Analytics for Fraud Coalition Prediction in Malaysia. In: IEEE. 2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE). [S.l.: s.n.], 2021. v. 6, p. 1–6.

- MOHER, David et al. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. **Annals of internal medicine**, American College of Physicians, v. 151, n. 4, p. 264–269, 2009.
- MORA-CANTALLOPS, Marçal et al. Traceability for trustworthy AI: a review of models and tools. **Big Data and Cognitive Computing**, MDPI, v. 5, n. 2, p. 20, 2021.
- MOREAU, Luc; GROTH, Paul. **Provenance: an introduction to PROV**. [S.l.]: Springer Nature, 2022.
- MUÑOZ-CANCINO, Ricardo; RÍOS, Sebastián A. Data-Driven Transparency: Machine Learning and Social Network Analysis for Corruption Detection in Public Procurement. **Procedia Computer Science**, Elsevier, v. 270, p. 1788–1795, 2025.
- MURIKAH, Wilberforce; NTHENGE, Jeff Kimanga; MUSYOKA, Faith Mueni. Bias and Ethics of AI Systems Applied in Auditing-A Systematic Review. **Scientific African**, Elsevier, e02281, 2024.
- NAGITTA, Pross Oluka et al. Human-centered artificial intelligence for the public sector: The gate keeping role of the public procurement professional. **Procedia Computer Science**, Elsevier, v. 200, p. 1084–1092, 2022.
- NAI, Roberto; FATIMA, Ishrat, et al. AI Applied to the Analysis of the Contracts of the Italian Public Administrations. In: CEUR. PROCEEDINGS of the Italia Intelligenza Artificiale-Thematic Workshops co-located with the 3rd CINI National Lab AIIS Conference on Artificial Intelligence (Ital IA 2023). [S.l.: s.n.], 2023. P. 255–260.
- NAI, Roberto; MEO, Rosa, et al. Public tenders, complaints, machine learning and recommender systems: a case study in public administration. **Computer Law & Security Review**, Elsevier, v. 51, p. 105887, 2023.
- NAI, Roberto; SULIS, Emilio; MEO, Rosa, et al. Public procurement fraud detection and artificial intelligence techniques: a literature review. In: CEUR-WS. COMPANION Proceedings of the 23rd International Conference on Knowledge Engineering and Knowledge Management. [S.l.: s.n.], 2022. P. 1–13.
- NAM, Hyundong; NAM, Taewoo; KIM, Songeun. Identifying the determinants of platform-based e-government service use. **Journal of Global Information Management (JGIM)**, IGI Global Scientific Publishing, v. 32, n. 1, p. 1–21, 2024.

- NIESSEN, Maria Elisabeth Kehler; PACIELLO, Julio Manuel; FERNANDEZ, Juan Ignacio Pane. Anomaly Detection in Public Procurements using the Open Contracting Data Standard. In: IEEE. 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG). [S.l.: s.n.], 2020. P. 127–134.
- NWAIMO, CHIOMA SUSAN; OLUOHA, OLUCHUKWU MODESTA; OYEDOKUN, OYEWALE. Big data analytics: technologies, applications, and future prospects. **Iconic Research and Engineering Journals**, v. 2, n. 11, p. 411–419, 2019.
- OKO-ODION, Courage. Ai-driven risk assessment models for financial markets: Enhancing predictive accuracy and fraud detection. **International Journal of Computer Applications Technology and Research**, v. 14, n. 04, p. 80–96, 2025.
- OLIVEIRA, Fernando Henrique Moura de. Quality concerns in public procurement data. **Programa de Pós-Graduação em Ciência da Computação - Universidade Federal de Sergipe**, Pós-Graduação em Ciência da Computação, 2024.
- OOSTHOEK, Koen. Public procurement in the European Union: Transparent and Fair? An evaluation of the effectiveness of directives 2014/23, 2014/24 and 2014/25 on indicators of transparency and corruption. **Romanian Journal of Political Sciences**, Societatea Academică Română (SAR), v. 20, n. 2, p. 30–61, 2020.
- PAGLIERI, Luigina; COSTUMATO, Lorenzo; BONOMI SAVIGNON, Andrea. Does artificial intelligence improve social equity in public services? A systematic literature review on opportunities and pitfalls. **International Journal of Public Sector Management**, Emerald Publishing Limited, p. 1–23, 2025.
- PANAGIOTOPOULOS, Panos; KLIEVINK, Bram; CORDELLA, Antonio. **Public value creation in digital government**. v. 36. [S.l.]: Elsevier, 2019. P. 101421.
- PEFFERS, Ken et al. Design science research evaluation. In: SPRINGER. INTERNATIONAL conference on design science research in information systems. [S.l.: s.n.], 2012. P. 398–410.
- POMPEU, Marcos Leno Ferreira; FILHO, Raimir Holanda. Public Procurement Collusion Identification Based on GraphSAGE Algorithm. In: SPRINGER. INTERNATIONAL Conference on Complex Networks and Their Applications. [S.l.: s.n.], 2024. P. 28–36.
- POTIN, Lucas et al. Pattern mining for anomaly detection in graphs: Application to fraud in public procurement. In: SPRINGER. JOINT European Conference on Machine Learning and Knowledge Discovery in Databases. [S.l.: s.n.], 2023. P. 69–87.

POWER, Michael. The apparatus of fraud risk. **Accounting, organizations and society**, Elsevier, v. 38, n. 6-7, p. 525–543, 2013.

PURVES, Duncan; DAVIS, Jeremy. Public trust, institutional legitimacy, and the use of algorithms in criminal justice. **Public Affairs Quarterly**, University of Illinois Press, v. 36, n. 2, p. 136–162, 2022.

PURWANTO, Agus; EMANUEL, Andi Wahju Rahardjo. Data analysis for corruption indications on procurement of goods and services. In: IEEE. 2020 3rd International Conference on Information and Communications Technology (ICOIACT). [S.l.: s.n.], 2020. P. 56–60.

RABUZIN, Kornelije; MODRUSAN, Nikola. Prediction of Public Procurement Corruption Indices using Machine Learning Methods. In: KMIS. [S.l.: s.n.], 2019. P. 333–340.

RACHMAT, Sulaeman et al. Fraud in Public Procurement: Governance, Internal Supervision and Political-Economic Challenges in the Indonesian Context. **PUBLIC GOVERNANCE ADMINISTRATION AND FINANCES LAW REVIEW**, v. 10, n. 2, p. 115–136, 2025.

RATHORE, M Mazhar et al. Exploiting IoT and big data analytics: Defining smart digital city using real-time urban data. **Sustainable cities and society**, Elsevier, v. 40, p. 600–610, 2018.

REBUGLIO, Massimo; OTTAVIANI, Filippo Maria; DE MARCO, Alberto. Recordkeeping for project management information system in public procurement: an action research. **Records Management Journal**, Emerald Publishing Limited, 2025.

RENDON, Rene G; RENDON, Juanita M. Auditability in public procurement: An analysis of internal controls and fraud vulnerability. **International Journal of Procurement Management**, Inderscience Publishers (IEL), v. 8, n. 6, p. 710–730, 2015.

RIBEIRO, Marco Tulio; SINGH, Sameer; GUESTIN, Carlos. " 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. [S.l.: s.n.], 2016. P. 1135–1144.

RIYAD, Berraida et al. The Artificial Intelligence and Public Procurement. In: IEEE. 2024 IEEE 15th International Colloquium on Logistics and Supply Chain Management (LOGISTIQUA). [S.l.: s.n.], 2024. P. 1–6.

- RODRÍGUEZ, Manuel J García et al. Collusion detection in public procurement auctions with machine learning algorithms. **Automation in Construction**, Elsevier, v. 133, p. 104047, 2022.
- RUPPRECHT, Lukas et al. Improving reproducibility of data science pipelines through transparent provenance capture. **Proceedings of the VLDB Endowment**, VLDB Endowment, v. 13, n. 12, p. 3354–3368, 2020.
- RUSTIARINI, Ni Wayan; NURKHOLIS, Nurkholis; ANDAYANI, Wuryan. Why people commit public procurement fraud? The fraud diamond view. **Journal of public procurement**, Emerald Publishing Limited, v. 19, n. 4, p. 345–362, 2019.
- SAFAROV, Igbal. Institutional dimensions of open government data implementation: Evidence from the Netherlands, Sweden, and the UK. **Public Performance & Management Review**, Taylor & Francis, v. 42, n. 2, p. 305–328, 2019.
- ŞAHİN, Emrullah; ARSLAN, Naciye Nur; ÖZDEMİR, Durmuş. Unlocking the black box: an in-depth review on interpretability, explainability, and reliability in deep learning. **Neural Computing and Applications**, Springer, p. 1–107, 2024.
- SAMPAIO, Igor; BERNARDINI, Flávia; VITERBO, José, et al. Public Procurement Risk Indicators from Open Government Data and Provenance Model. English. **EGOV-CeDEM-ePart 2026**, 2026. DOI: 10.59490/6a91adc10fd2bd55cd254870. Available from:
<<https://dapp.orvium.io/deposits/6a91adc10fd2bd55cd254870/view>>.
- SAMPAIO, Igor; FONTES, Sergio, et al. Enhancing Transparency through Explainable Artificial Intelligence: An Exploratory Analysis on Collusion and Corruption Scenario in Digital Government. In: PROCEEDINGS of the 25th Annual International Conference on Digital Government Research. [S.l.: s.n.], 2024. P. 52–62.
- SAMPAIO, Igor Garcia Ballhausen; BERNARDINI, Flávia Cristina; VITERBO, José. Challenges in Addressing the Ethical Aspects of Artificial Intelligence to Detect Fraud in Public Procurement Processes. In: SBC. CONFERÊNCIA Latino-Americana de Ética em Inteligência Artificial. [S.l.: s.n.], 2024. P. 13–16.
- SAMPAIO, Igor Garcia Ballhausen; DE OLIVEIRA ANDRADE, Eduardo, et al. Trustworthy AI in public administration: The PRO-Trust pipeline for ethical fraud detection in public procurement. **Government Information Quarterly**, v. 43, n. 3, p. 102157, 2026. ISSN 0740-624X. DOI:
<https://doi.org/10.1016/j.giq.2026.102157>. Available from:
<<https://www.sciencedirect.com/science/article/pii/S0740624X26000547>>.

- SANTOS, Franklin Brasil; SOUZA, Kleberson Robert de. **Como combater a corrupção em licitações**. [S.l.]: Editora Forum, 2016.
- SCHLIMBACH, Ricarda et al. A teaching framework for the methodically versatile DSR education of master's students. **Journal of Information Systems Education**, ISCAP, Information Systems and Computing Academic Professionals, North . . ., 2023.
- SCHMITZ, Andreas et al. Architecture Interoperability through Semantic Modelling: Domain-driven data specification in public procurement. **ECIS 2025 Proceedings**, 2025.
- SELIM, Ahmed M; YOUSEF, Pasent HA; HAGAG, Mohamed R. Risk allocation for infrastructure projects by PPPs-under environmental management and risk assessment mechanisms. **International Journal of Risk Assessment and Management**, Inderscience Publishers (IEL), v. 22, n. 1, p. 89–108, 2019.
- SETYAWAN, Adhitya Chandra. Enhancing public service delivery through digital transformation: A study on the role of E-government in modern public administration. **Global International Journal of Innovative Research**, v. 2, n. 10, p. 2439–2453, 2024.
- SHAELOU, Stéphanie Laulhé; RAZMETAeva, Yulia. Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems: shaping the digital legal order while upholding Rule of Law principles and European values. In: SPRINGER. ERA Forum. [S.l.: s.n.], 2023. v. 24, p. 567–587.
- SHAHRIAR, Sakib et al. A survey of privacy risks and mitigation strategies in the artificial intelligence life cycle. **IEEE Access**, IEEE, v. 11, p. 61829–61854, 2023.
- SHARMIN, Shabnam; CHOWDHURY, Rakibul Hasan. Digital transformation in governance: The impact of e-governance on public administration and transparency. **Journal of Computer Science and Technology Studies**, v. 7, n. 1, p. 362–379, 2025.
- SIGFRIDS, Anton et al. How should public administrations foster the ethical development and use of artificial intelligence? A review of proposals for developing governance of AI. **Frontiers in Human Dynamics**, Frontiers Media SA, v. 4, p. 858108, 2022.
- SIMMHAN, Yogesh L; PLALE, Beth; GANNON, Dennis, et al. A survey of data provenance techniques. **Computer Science Department, Indiana University, Bloomington IN**, v. 47405, p. 69, 2005.

SINGH, Jatinder; COBBE, Jennifer; NORVAL, Chris. Decision provenance: Harnessing data flow for accountable systems. **IEEE Access**, IEEE, v. 7, p. 6562–6574, 2018.

SIROREI, James K. **Agent based fraud detection and reporting in public e-procurement**. 2018. PhD thesis – University of Nairobi.

SOYLU, Ahmet et al. Data quality barriers for transparency in public procurement. **Information**, MDPI, v. 13, n. 2, p. 99, 2022.

SPULBAR, Lucian-Florin. Legal frameworks for AI-driven markets and their challenges and opportunities in the digital economy. **Revista de Științe Politice. Revue des Sciences Politiques**, Editura Universitaria Craiova, n. 86, p. 288–304, 2025.

SUSAR, Deniz; AQUARO, Vincenzo. Artificial intelligence: Opportunities and challenges for the public sector. In: PROCEEDINGS of the 12th international conference on theory and practice of electronic governance. [S.l.: s.n.], 2019. P. 418–426.

TAHMINA, Ahmed; NAIMA, Jannatul. Detection and analysis of probable earnings manipulation by firms in a developing country. **Asian Journal of Business and Accounting**, v. 9, n. 1, p. 59–82, 2016.

TALUKDER, Khairul Alam. The impact of data-driven decision support systems on governance and policy implementation in US institutions. **ASRC Procedia: Global Perspectives in Science and Scholarship**, v. 1, n. 01, p. 994–1030, 2025.

TAS, Bedri Kamil Onur. A machine learning approach to detect collusion in public procurement with limited information. **Journal of Computational Social Science**, Springer, p. 1–23, 2024.

TAS, Bedri Kamil Onur. Weak supervision can help detecting corruption in public procurement. In: SPRINGER. PROCEEDINGS of SAI intelligent systems conference. [S.l.: s.n.], 2022. P. 548–555.

TÁTRAI, Tünde; NÉMETH, Anita. Improving red flag instruments for public procurement. In: SPRINGER. ERA Forum. [S.l.: s.n.], 2018. v. 19, p. 267–285.

THAI, Khi V. International public procurement: Concepts and practices. In: INTERNATIONAL handbook of public procurement. [S.l.]: Routledge, 2017. P. 1–24.

THAI, Khi V. Public procurement re-examined. **Journal of public procurement**, Emerald Publishing Limited, v. 1, n. 1, p. 9–50, 2001.

TISHCHENKO, Ekaterina. Special Aspects of Criminal Activity in the Field of Public and Municipal Procurement. **Indian Journal of Science and Technology**, v. 9, n. 46, p. 107531–107531, 2016.

- TORRES BERRU, Yeferson et al. Artificial intelligence techniques to detect and prevent corruption in procurement: a systematic literature review. In: SPRINGER. INTERNATIONAL Conference on Applied Technologies. [S.l.: s.n.], 2020. P. 254–268.
- TORRES-BERRU, Yeferson; LÓPEZ BATISTA, Vivian Felix. Data and text mining for the detection of fraud in public contracts: A case study of Ecuador's official public procurement system. In: SPRINGER. DOCTORAL Symposium on Information and Communication Technologies-DSICT. [S.l.: s.n.], 2022. P. 116–127.
- TORRES-BERRU, Yeferson; LOPEZ-BATISTA, Vivian F; ZHINGRE, Lorena Conde. A Data Mining Approach to Detecting Bias and Favoritism in Public Procurement. **Intelligent Automation & Soft Computing**, v. 36, n. 3, 2023.
- TÓTH, Bence; FAZEKAS, Mihály, et al. Toolkit for detecting collusive bidding in public procurement. **With examples from Hungary**, 2014.
- TÓTH, István János; HAJDU, Miklós. Corruption risk and EU funding in public procurement across EU member states, 2007–2023. **Acta Oeconomica**, Akadémiai Kiadó Budapest, v. 75, n. 4, p. 485–518, 2025.
- ULLOA, Sthefano et al. Building a Generalized Framework for Analyzing Public Procurement Data from the Kapak Database. In: IEEE. 2025 IEEE Ninth Ecuador Technical Chapters Meeting (ETCM). [S.l.: s.n.], 2025. P. 1–6.
- VELASCO, Rafael B et al. A decision support system for fraud detection in public procurement. **International Transactions in Operational Research**, Wiley Online Library, v. 28, n. 1, p. 27–47, 2021.
- VETRÒ, Antonio et al. Open data quality measurement framework: Definition and application to Open Government Data. **Government Information Quarterly**, Elsevier, v. 33, n. 2, p. 325–337, 2016.
- WEINGÄRTNER, Tim et al. Prototyping a smart contract based public procurement to fight corruption. **Computers**, MDPI, v. 10, n. 7, p. 85, 2021.
- WEISHAAR, Stefan. **Cartels, competition and public procurement: Law and economic approaches to bid rigging**. [S.l.]: Edward Elgar Publishing, 2013.
- WERDER, Karl; RAMESH, Balasubramaniam; ZHANG, Rongen. Establishing data provenance for responsible artificial intelligence systems. **ACM Transactions on Management Information Systems (TMIS)**, ACM New York, NY, v. 13, n. 2, p. 1–23, 2022.

WESTERSKI, Adam et al. Explainable anomaly detection for procurement fraud identification—lessons from practical deployments. **International Transactions in Operational Research**, Wiley Online Library, v. 28, n. 6, p. 3276–3302, 2021.

WOHLIN, Claes et al. **Experimentation in software engineering**. [S.l.]: Springer, 2012. v. 236.

XAVIER, Otávio Calaça et al. Tax evasion identification using open data and artificial intelligence. **Revista de Administração Pública**, SciELO Brasil, v. 56, p. 426–440, 2022.

YEUNG, Karen. Recommendation of the council on artificial intelligence (OECD). **International legal materials**, Cambridge University Press, v. 59, n. 1, p. 27–34, 2020.